Chapter 8

Investigative-Reporting Agencies

A common denominator of many record-keeping institutions examined in preceding chapters is their dependence on support organizations to gather and maintain information that has protective value. Credit and inspection bureaus, independent credit-card authorization and check-guarantee services, the Medical Information and Loss Index Bureaus of the insurance industry, all exist to protect their clients from the individual who falsifies or fails to reveal significant information that could alter the credit, insurance, or employment decision to be made about him.

Some of these support organizations are simply clearinghouses that save their clients from having to contact one another directly. Credit-card authorization services and the Medical Information Bureau are prime examples. As explained in Chapters 2 and 5, the information in their files comes from their clients; they do not have their own independent sources. Other support organizations, however, use investigative techniques to gather the information they report about individuals. Although they, too, maintain files, they develop their information initially through interviews and inquiries of neighbors, business associates, employers, and other record-keeping institutions.

The purpose of this chapter is threefold: (1) to describe the practices of the various investigative support organizations so that their relationship to the decision-making processes of their clients may be clearly appreciated; (2) to explain in one place how the Commission's recommendations in other chapters address problems that the activities of investigative support organizations create; and (3) to outline for further study some areas the Commission has not been able to address but considers worthy of examination.

The chapter begins with an overview of the activities of two types of investigative support organizations on which the Commission was able to develop substantial detail: the *inspection bureaus* whose reports are primarily used in insurance underwriting; and the *private-investigative agencies* that principally make background inquiries about individuals for employers. This is followed by a section on investigative services performed in connection with the settlement of insurance claims or for an employer who believes it has internal security problems. Finally, the concluding sections summarize the Commission's recommendations in other chapters which affect the activities of investigative-reporting agencies and suggest problem areas that, in the Commission's opinion, merit further examination.

CamScanner

THE INSPECTION BUREAU: AN OVERVIEW

In insurance underwriting the company and the individual consumer strive for different ends—the individual, to acquire protection at the lowest possible cost; the company, to minimize its risk and control claims and administrative overhead. Moreover, because most insurance is sold through an agent field force that derives its income from commissions, a company wants some kind of independent check on the applicants or insureds and the information about them that agents submit. Inspection bureaus exist in large measure to satisfy these company needs for information about the individual with whom it has or proposes to have an insurance relationship.

The inspection bureau industry, like the credit-reporting business, is a concentrated one. Equifax Services, the industry giant, prepares over 15 million inspection reports each year.[1]

Originally insurance companies did their own inspection work. As business grew, however, multiplying the number of necessary inspections, they began to rely more and more on the bureaus. Because an inspection bureau can serve more than one company client in a given geographic area, it saves all its company clients money. Furthermore, when an insurance company orders an inspection report, it is not just purchasing an investigative capability to develop and verify information; it is also purchasing access to an existing reservoir of information on individuals who have previously been investigated, and this too constitutes an important cost-saving factor.

The services inspection bureaus perform are labor-intensive. While credit bureaus may profitably exploit the speed and efficiency of modern information-processing technology, it is hard to see how the computer can replace the inspection bureau field worker who specializes in interviewing neighbors and associates. Inspection bureaus are aware of this and, consequently, place a premium on the productivity of individual investigators. Pay scales are comparatively low. Costs must be kept down lest the companies lose their incentive to use bureau services. The general level of education and training required can be modest.[2] Inspectors are often part-time students, off-duty policemen, housewives, and retired persons. Advertisements for investigators indicate that to qualify, an individual need only have a high school diploma and a car.[3] Obviously, pressures to produce,

---

[1] Testimony of Equifax, Inc., *Credit Reporting and Payment Authorization Services*, Hearings before the Privacy Protection Study Commission, August 3, 1976, p. 163 (hereinafter cited as "Credit Reporting Hearings").

[2] The experience level and turnover rate of inspection bureau personnel is a matter of some question. Equifax, Inc., testified that about 64 percent of its field representatives had some college training, with approximately 25 percent holding at least a bachelor's degree, and that the average field representative had almost 12 years of company experience. (Credit Reporting Hearings, August 3, 1976, p. 163). However, a former supervisor with 15 years experience at Equifax asserted in a letter to the Senate Banking Committee that Equifax commonly employed investigators on a part-time basis who lacked the "investigative training for the types of decisions which they must make," a problem which was further complicated by an "extremely high" turnover rate. (Letter from Daniel P. Reiter to the Senate Banking Committee, August 5, 1976.)

[3] *Miami Herald*, June 11, 1974, p. 18-e.

CamScanner

coupled with low salary scales, can easily affect the quality of an inspection bureau's product.

Types of Information Collected

An insurance company generally uses an inspection report to help it answer two related types of questions: (1) whether to grant or continue coverage; and (2) if coverage is to be granted or continued, what is the proper price to charge. That is, in the absence of information it considers derogatory, an insurance company will normally proceed with the coverage requested, concerning itself only with items of information that may affect the premium it will charge. Or, if it has already written a policy, derogatory information in a subsequently provided report may be used as the basis for cancelling or refusing to renew the policy or for altering the premium. Automobile insurance, for example, almost always becomes effective immediately upon filing an application with a company or its agent. However, information in an inspection report the insurer subsequently acquires may cause it to charge the consumer a higher premium than he originally anticipated or cause the insurer to terminate the policy altogether.[4]

Because Equifax Services accounts for a major proportion of the inspection bureau business,[5] a review of its investigative manuals[6] and its report forms can offer substantial insight into the kinds of information insurance underwriters consider "adverse." Because of Equifax's dominant position in the inspection industry, a survey of its major reporting services should also afford a good understanding of typical bureau practices.

In addition to extensive questions covering the identity of the individual, details as to his past employment, driving record, finances, insurance history (including special ratings or previous declinations), Equifax inspectors are asked in different reports to respond "yes" or "no," and if "yes," to provide greater detail on questions, such as the following:

- Use alcohol? (If "yes," answer: (1) What? (2) How often? (3) How many? (4) Where? (5) Over what period of time?)
- Use(d) marijuana?

[4] See Chapter 5 for a discussion of the insurance underwriting process.

[5] According to the Federal Trade Commission, in 1970 the Retail Credit Company (Equifax, Inc.) produced approximately 26,000,000 consumer reports for credit, personnel, and other purposes, resulting in revenues in excess of $136,000,000. (United States of America before the Federal Trade Commission, in the matter of Retail Credit Company, Docket No. 8920, initial decision February 10, 1976, p. 10). In his opening statement in 1974 Senate hearings on the credit-reporting industry, Senator William Proxmire (D.-Wisc.) stated that ". . . the Retail Credit Company accounts for over two-thirds of the investigative reporting industry, and other firms within the industry have closely followed the practices and procedures of Retail Credit." (*Credit Reporting Abuses*, Hearings before the Subcommittee on Consumer Credit of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 93d Congress, 2d Session, 1974, p. 1).

[6] Equifax, Inc., "Property Lines Manual," May 1975; "Life and Income Protection Manual," November 1974; and "Employment Reports Manual," March 1976.

CamScanner

- Use(d) narcotics, sedatives, depressants, stimulants, or hallucinogens?
- How was worth acquired? (Inherited, accumulated, or speculation)
- If other than married, does applicant reside with another person?
- Anything adverse about reputation, life style, or home environment?
- Do any of the following apply? Unfair business practices? Heavy debts? Domestic trouble?
- Reputation of business questionable?
- Any evidence of job instability?
- Personal reputation or associates questionable?[7]

While a "yes" answer to any of these questions is explained on the back of the form, the yes-no portion serves to "flag" items that meet the receiving insurer's concept of "adverse" information. (Inspection bureaus commonly develop different report forms for the different types of insurance each underwrites.)

Arguably, some of the information the inspection bureau's clients consider "adverse," "actionable," "declinable," "pertinent," or "significant," does not indicate an above-average insurance risk. While there are broad areas of overlap between what a community may hold to be negative characteristics and what may constitute a demonstrable risk to an insurer (for example, an alcoholic who is held in low public regard because of his behavior is also avoided by an automobile insurer), there are socially unacceptable traits that may have no bearing at all on risk in a particular line of insurance. A bearded, blue-jeaned resident of a small town might encounter some difficulty if his neighbors were asked to evaluate his "reputation" or "trustworthiness." Yet, the personal characteristics that set him apart may be of no importance in underwriting auto, life, or homeowner's insurance. An inspection report, however, does not make these fine distinctions, nor can it take account of the prejudices or other idiosyncracies of the people who are asked to make such subjective judgments, including, in many cases, the investigator himself.

Information Collection Methods

As indicated earlier, the use of personal interviews to gather information about an individual is one of the distinguishing characteristics of an investigative support organization. Inspection bureau field representatives generally interview an applicant's neighbors and business associates or fellow employees, as well as other sources that may be suggested along the way. As to the last, an interview with the applicant himself can be one of the most important sources of leads.

Unless specifically prohibited from doing so by the insurance company, or unless the bureau's own past experience with the applicant

[7] *Ibid.*

indicates that he will not be cooperative, an inspection bureau may attempt to interview him and some insurance companies require the inspection bureau to do so. Indeed, in some instances an inspection bureau does no more than verify information in the application directly with the applicant.

According to Equifax internal documents, the applicant can provide the following types of information in a direct interview:

- Health: history, attending/personal physicians, height/weight/waist measurement, impairments, smoking.
- Finances: exact income and worth figures or very close estimates. Personal financial statements.
- Occupation: details on employment status, business history, foreign travel, part-time jobs.
- Duties: a precise description of work performed.
- Identity: thorough identification of the applicant.
- Military: past or present connections.
- Spare Time: sports, hobbies, flying, club affiliations.
- Driving: record of accidents and violations.
- Drinking: description of drinking habits.
- Drugs: present or past use.
- Criminal Record: arrests and convictions.
- Other Coverage: amounts and carriers. Previous ratings and declinations.
- Financial Problems: details of problems or tips to same.
- References: name of personal acquaintances, bankers, permission to see accountants and attorneys.[8]

Inspection bureaus prefer that all interviews be conducted in person. Interviewing by telephone is discouraged, unless the purpose of the interview is to verify information obtained in an earlier investigation. Apparently, however, it is not strongly discouraged since the testimony of several former field representatives before congressional committees indicates that telephone interviews are, in fact, widely used for the simple reason that they save time.[9]

In an April 1975 *New Yorker* article, "Anything Adverse?," the Equifax "Manager Manual" was quoted on the techniques used to elicit

[8] Equifax, Inc., "Life and Income Protection Manual," November 1974, p. D-20.

[9] *Credit Reporting Abuses*, Hearing before the Subcommittee on Consumer Credit of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 93d Congress, 2d Session, 1974.

CamScanner

information in an interview. The field representative "must not be afraid to ask personal questions"[10] and "should be sufficiently suspicious by nature to derive satisfaction from tracking down leads and developing the facts."[11] To this end:

> the top-notch Field Representative should be highly sensitive to the more subtle clues in the remarks of his sources and other behavior, perceiving their implications and adapting his own approach and conversation accordingly . . . . A sense of humor [will prove to be] a powerful instrument in the development of a warm, friendly relationship with sources. In fact some of the most pertinent personal information is sandwiched in between homey remarks and other small talk.[12]

According to the Equifax "Field Representative Manual," the interviewer should:

> . . . proceed from the impersonal to the personal. People do not readily talk to strangers about the personal reputation and morals of their friends and acquaintances. However, after first talking about impersonal areas (identity, employment, and health), they have less hesitancy to cover more personal matters.[13]

In addition to learning this basic interview strategy, the interviewer is instructed to ask open-ended questions, such as "How is he regarded?" instead of, "Is he well regarded?"; or "How much does he drink?," not "Does he drink?"[14] Because inspection field representatives are in the business of collecting rather than distributing information, all are strongly advised not to transmit to any sources the information acquired from other ones. In many cases, moreover, the name of the client, i.e., the insurance company, is not to be given. Indeed, in some cases, the source being interviewed will not be aware, even in a general sense, of the purpose of the interview.

Record searches are the second method by which inspection bureau field representatives collect information. Many records held by city, county, State, and Federal agencies are open to public inspection. Depending upon the locality, these may include police arrest blotters, civil and criminal court records, motor vehicle accident reports, records of driving convictions, and possibly even welfare rolls or other records concerning contacts with social service agencies.[15] Adverse information obtained from public records is of particular value to an inspection bureau. In addition to being unfavorable and, therefore, valuable to the bureau's clients, such information, in contrast to information obtained from neighbors or associates, does not require

---

[10] Equifax, Inc., "Manager Manual," as cited by Thomas Whiteside, "Anything Adverse?," *New Yorker*, April 21, 1975, p. 54.
[11] *Ibid.*
[12] *Ibid.*
[13] Equifax, Inc., "Field Representative Manual," April 1973, p. 29.
[14] *Ibid.*
[15] Equifax, Inc., "Claim Reports Manual," November 1975, pp. C-15 - C-17.

CamScanner

reverification under the Fair Credit Reporting Act (FCRA) when carried forward from one report to another (except where the report is for employment purposes). *[15 U.S.C. 1681l]* Further, public-record information alone does not meet the FCRA definition of a "consumer investigative report." *[15 U.S.C. 1681k]* Thus, a report containing information about anything from character and morals to business reputation and domestic difficulties can be prepared solely on the basis of public records without the individual who is the subject of it receiving the prior notification the FCRA otherwise requires.

Mindful of this, some inspection bureaus are now encouraging their clients to depend more upon information that can be gleaned from public records than on the "subjective information" heretofore gathered from neighbors and associates. As the President of O'Hanlon Reports, Inc., described the current situation to the Commission:

> Our business [has changed] drastically in the past three years from a time when subjective reports constituted as much as 80 to 85 percent of our business . . . . Today, subjective reports are less than 40 percent . . . and we do everything we can do to accomplish the point of getting the underwriting people and the insurance companies to allow us to make the short-form classification, the short-form dwelling reports, and so on, that do not require subjective information . . . . That is the future of the inspection business . . . . Use these other reports and stop making everybody liable for all kinds of problems . . . .[16]

As indicated in Chapter 2, credit reports are an important source of public-record information for inspection bureaus. Most inspection bureaus (like most private investigative firms) are eligible to subscribe to credit bureaus and some of the larger inspection bureaus own one or more.[17] In addition, if the inspection bureau has a signed authorization in hand, it can often get banks and accountants to make or confirm a reasonably accurate estimate of an individual's income. For underwriting life or disability insurance on self-employed individuals, this is particularly helpful as estimates of their income or worth might otherwise be difficult to obtain.

Besides interviews and record searches, inspection bureaus also use their own files as a basic source of information. In fact, in some cases, their own files are the only source they use. To get an investigation started, the insurance company must provide basic identifying information on the individual, and may, in addition, ask the bureau to verify other items the individual himself has already provided on the application form.

Equifax's Chairman told the Commission that at any given time his company will be maintaining files in its local offices on up to 25 percent of a

---

[16] Testimony of O'Hanlon Reports, Inc., Credit Reporting Hearings, August 3, 1976, pp. 142-43.

[17] Equifax, Inc., and Hooper-Holmes Bureau, Inc., own and operate major credit bureaus. See, for example, Testimony of Equifax, Inc., Credit Reporting Hearings, August 3, 1976, p. 150.

CamScanner

community's inhabitants with the nationwide total of files maintained being in the order of 39 million.[18] Because investigator expenses are the largest single contributor to the cost of preparing an inspection report, a bureau's files are a valuable cost-saving resource. The Fair Credit Reporting Act allows a bureau to report without verifying any information it has gathered through personal interviews within the previous three months, as well as any information it has obtained from public records. Older material must be reverified before it can be included in a current report, but it can also be used as leads to possible new information. This situation, plus the pressures on an investigator to work as quickly as possible, explains why the same adverse information can be reported again and again, and why a report containing false information can create recurring problems for an individual over a period of years.

It also explains why inspection bureaus tend to retain derogatory information in their files. Equifax policy calls for the destruction every thirteen months of reports made to life, auto, and property insurers, unless " . . . serious significant information is involved," in which case company manuals direct that such reports be kept for ten years. Motor vehicle reports are normally kept for five years from the date they are acquired, unless they are seriously unfavorable, in which case they, too, will be kept for ten years.[19] Since the FCRA imposes no time limit on the retention, as opposed to the reporting, of such adverse information, there is nothing other than cost to keep it from being kept in a bureau's files forever.

Production Pressures: Incentives for Invention

In February 1974, Mark S. Brodie testified before the Senate Banking, Housing, and Urban Affairs Committee that when he had worked briefly as a part-time Equifax investigator the previous year, his average workload was 15 cases per four-hour day, or about 16 minutes a case. Brodie described a procedure known in his office as "zinging":

> A zing means you do nothing. You do not contact the investigatee. One does not go out on the street . . . he utilizes whatever information was supplied by the insurance company, and hopefully, looks up the insured in the phone book to assure that he lives there; then you just fill in the form.[20]

Another investigator, Dick Riley, who worked fifteen years for Equifax, also testified to the same practice, known in his office as "the crystal-ball

[18] Credit Reporting Hearings, August 3, 1976, p. 171.

[19] Equifax, Inc., "Reference File Information—How to Destroy and Expert Files," (Form 1912), June 1975.

[20] *Credit Reporting Abuses*, Hearing before the Subcommittee on Consumer Credit of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 93d Congress, 2d Session, 1974, p. 11.

CamScanner

system," which "consists of quoting old reports, looking at [the information on] an inquiry, and determining that the individual 'looks okay.'"[21] Of course, "zinging" and "the crystal-ball system" have their pitfalls. Brodie told of one report that cited a source at a certain address which turned out to be a parking lot, and related an incident where an investigator "zinged" a report on an individual who was no longer living. Such practices are flagrant violations of corporate policy, but they apparently do occur.

Perhaps the most controversial aspect of inspection bureau operations is their use of production schedules for measuring the performance of field representatives. Discussions of production schedules usually begin with the proposition that it is impossible to speak of an "average" number of reports that can be completed by a "typical" field representative. Nevertheless, inspection bureaus do establish performance standards for their field representatives and successfully communicate the rewards and sanctions for exceeding or failing to meet them.[22]

Equifax has periodically conducted studies to determine the level of effort necessary to complete various types of reports.[23] In testimony submitted to the Commission,[24] Equifax representatives stated that regular life and automobile reports, the firm's two basic reporting services, are used to develop comparative measures of the time and effort that can be expended on its other reports and still produce a profit. Exceptions to these measures are allowed if a field representative has a preponderance of more (or less) complicated reports to prepare. Nonetheless, the economics of the firm's reporting services are such as to place constant pressure on management, and thus presumably on each field representative, to complete reports as quickly as possible. For its high-volume, low-cost reporting services, time is money for a firm like Equifax. Hence, the more reports that are produced within a given period of time, the more likely that the firm will be able to turn a profit without having to raise its prices.

In addition to the pressure to keep the number of reports high, critics have also alleged that Equifax keeps track of the amount of adverse information each report contains and that these statistics are translated by Equifax management and field workers into "adverse information quotas." The evidence on this point is confusing, in large measure because discussions of it in public forums have invariably failed to distinguish clearly between pressures to push up the number of reports produced and pressures to keep the *quality* of reports at acceptable levels. At one time Equifax apparently did keep statistics on the gross percentages of "protective" and "declinable" information in reports emanating from each field office. A December 15, 1972 memorandum from the Vice President for Operations, Southern Pacific Region, congratulates regional field office managers for having finished "in the upper third grouping in both total protective and

[21] *Ibid.*, p. 6.

[22] See Supplementary Statement of Retail Credit Company (Equifax, Inc.), *Fair Credit Reporting Amendments of 1975,* Hearings before the Subcommittee on Consumer Affairs of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 94th Congress, 1st Session, 1975, pp. 233-35.

[23] *Ibid.*

[24] Written statement of Equifax, Inc., Credit Reporting Hearings, August 3, 1976, pp. 17-18.

percent declinable" in the second round of an intra-company survey called the "Life and Health Quality Profile." In addition, the memorandum went on to extol the "vast improvement" in both life and health and auto reporting "since they [sic] have been keeping this record back to 1968."[25] In sworn testimony before the Privacy Commission, however, Equifax representatives stated that "we no longer accumulate statistics concerning 'pertinent' information,"[26] and in a subsequent letter to the Commission indicated that they had formally ceased to do so in January 1976,[27] approximately eight months before testifying in the Commission's hearings. It has never been established, moreover, that competition among field offices, which the 1972 memorandum suggests the "pertinent information" statistics induced, was ever formally translated into adverse information quotas for individual field representatives. Nor need it have been.

One might well argue that the whole controversy over adverse information quotas misses the point by failing to recognize that adverse information is the inspection bureau's most salable product. Insurance companies have little use for innocuous commentary about applicants and policyholders. They are paying to find out whether there is anything about an individual which would warrant declining him or altering the premium he would otherwise be charged. From their point of view, it makes no difference whether "adverse" information is included in 10 or 30 or even 100 percent of the reports received. What they want is as thorough and accurate an investigation as they can get within the boundaries set by the price they are willing to pay. The proportions are irrelevant; the type of information and its quality are what counts.

It is true, of course, that both insurers and the investigative support organizations which service them share a less than rosy view of human nature. When asked if his firm's credibility would not be jeopardized if the amount of adverse information in its reports went down substantially over a period of time, Equifax's Chairman responded that in all probability it would "because we know the social behavior of our population is not improving that much."[28]

> . . . we know that if . . . [an investigator] works intelligently and carefully and conscientiously, . . . he is going to develop a rather substantial amount of information that we term as pertinent information, pertinent to the risk . . . . We have a rather homespun Executive Vice President who said that if you send a man to a blackberry field every day with a bucket and every day he came

[25] Equifax, Inc., "L & H [Life and Health] Quality Profile," Memorandum from Russell H. Beckett, Regional Vice President to Managers, December 15, 1972. Cited in *Fair Credit Reporting Act—1973*, Hearings before the Subcommittee on Consumer Credit of the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 93d Congress, 1st Session, 1973, p. 877.
[26] Written Statement of Equifax, Inc., Credit Reporting Hearings, August 3, 1976, p. 19.
[27] Letter from Equifax, Inc., to the Privacy Protection Study Commission, February 23, 1977.
[28] Credit Reporting Hearings, August 3, 1976, p. 235.

back with no blackberries, then you would notice that something was wrong.[29]

Such a statement, while neither proving nor disproving the quota allegation, makes a powerful point: that the underlying assumption of any inspection bureau investigation is that a certain amount of adverse information may be developed. This does not mean that adverse information *will* be developed in every instance but rather that an inspector should find adverse information on at least some applicants, because adverse information is assumed to be there to be discovered. If an inspector consistently finds nothing, or very little, the inevitable conclusion is that he has not done his job, not that the individuals he was assigned to investigate all happen to be sterling characters.

Understanding the natural emphasis of the inspection bureau's product also helps to understand a point made in the introduction to this report: that from a purist point of view, factual inquiries can involve more of an intrusion on an individual's personal privacy than subjective ones. The following February 1972 communication was directed to all Equifax field representatives:

Believe me -

It Makes the Difference

This Doesn't Tell the Story -
"Insured drinks to excess on weekends."
"Drinks to excess on special occasions."
"Drinks to feeling good and drives afterward."
"Drinks a few beers daily."
"Is criticized for being a heavy drinker."
"Used to drink a lot but quit."

We Haven't Done the Job Unless
We've Found Out and Reported -
What he drinks.
How often he drinks - daily, weekly, monthly, 2-3 a year?
How much he drinks -
If daily - how many, and where, and when?
If on weekends - every weekend, or most, or 1-2 a month?
If to excess - feeling good or loud and boisterous or intoxicated?
- how often - daily, weekly, monthly, 1-2 a month, 2-3 a year?
Where he drinks - home, tavern, lounge, club, parties, on the job?
When he drinks - evenings, lunch, on the way home from work?
How long - if he quit, specifically when and why?

[29] *Ibid.*, pp. 236-37.

Does he drive afterwards?[30]

At first glance, such an exhortation to further prying may seem patently offensive. When one compares the first set of inquiries (deemed inadequate) with the second (considered desirable), however, one realizes that the latter is far more factual in its orientation than the former. Whether an individual would fare better with an insurer if the factual details of his drinking behavior were manifest (the second set of questions), in lieu of purely subjective characterizations of it (the first set), will depend on the company he is dealing with and the type of insurance he is seeking. The important point to grasp, however, is that intrusions on personal privacy of the sort in which inspection bureaus engage usually begin with the criteria we, as a society, accept as proper ones for making decisions about people; and that so long as society countenances certain lines of inquiry by certain types of record-keeping institutions, questions as to how far a line of inquiry may properly go are largely aesthetic. Indeed, if one prefers that decisions be made on the basis of facts rather than subjective evaluations, one should logically prefer that the line of inquiry be quite detailed as a protection against drawing inaccurate inferences.

THE PRIVATE INVESTIGATIVE AGENCY: AN OVERVIEW

While an inspection report can be the sole basis for making an adverse insurance decision, the background investigations that private investigative agencies conduct for employers are just a part of the information that is taken into account in making a decision about an individual. In most hiring situations, the employer will interview the applicant directly, using the private investigator only to verify information to be used in making the decision. In some cases, however, the results of a background investigation can be the determining factor. For example, an employer may engage the services of a private investigative agency to find out if an applicant or employee has an unsavory background or reputation of which the employer is unaware; to see if there is criminal behavior in the applicant's background which may be relevant to the job applied for; or perhaps to check out an employment history that itself raises questions.

Another factor that distinguishes a preemployment investigation from the underwriting investigation conducted by an inspection bureau is that the criteria for accepting an applicant for employment are quite different from those governing insurance decisions. Whereas an insurance company makes a profit by accepting all comers who do not present unreasonable risk, there is a limit to the number of individuals an employer can hire. Hence, the employer must select the "best" candidate from the current pool of available applicants, which means, in turn, that the employer must rely on more information than just what an investigative agency gathers.

The information market that has evolved to meet the specific needs of employers also tends to be much more expensive than the market for

[30] Equifax, Inc., "It Makes a Difference," Memorandum from Quality Analysis Division to "Fellow Workers," February 1972.

inspection bureau services. Unless it is performed for a client already on retainer for other services, such as investigations of inventory losses or off-hour security guards, Pinkerton's, Inc., the nation's largest private investigative agency, will not accept a preemployment investigation which involves less than a day's billing. The average time billed by Per-Mar Security, a smaller firm, has been estimated at about a day and a half, and some investigations can run as long as three to four days.[31] From an employer's point of view, this can be advantageous. If an employer believes a particular individual is likely to do a good job, it does not want him disqualified by inaccurate or incomplete information, even if that means paying extra to assure a careful, thorough inquiry. Yet because the cost of gathering high-quality information can also outweigh its value in decision making, some employers have ceased to engage the services of investigative agencies, while others use them only for highly sensitive or key management positions.

In contrast to the inspection bureau workforce, the workforce of the private investigative agency is a skilled one. Instead of some use of part-time students, housewives, and retired persons, the private investigative agency tends to hire people who have previously worked for government law enforcement and investigative agencies. That is, it employs, on a full-time basis, a well trained individual who is acquainted with standard investigative practices and knows how to access public, as well as private, sources of information.[32] Moreover, because of the background of their employees, many private investigative firms do not require training programs for their new investigators, whereas most inspection bureaus provide basic instruction in interviewing and record-searching techniques.

Inspection bureaus also do a certain amount of preemployment work, although most of their reports, perhaps as many as 50 percent, are on applicants for employment in the insurance industry. Equifax Services, for example, does enough preemployment investigations to justify a separate division of the company. However, the reports it prepares are generally similar to its inspection reports, and the information in them is drawn from the same types of sources, including the same company files.[33] Equifax's instructions to investigators preparing preemployment reports parallel those to its field representatives preparing inspection reports, except for the extra stress they place on employment history and their observation that the applicant usually is not interviewed. Preemployment reports prepared by inspection bureaus also tend to be much cheaper than the ones prepared by private investigative firms, suggesting that they play a different role in the hiring decision or are ordered on a different level of applicant or employee. Thus, in the remainder of this section, the focus is on the more expensive private investigative report, save for a few instances in which comparisons with inspection bureau practices seem important enough to be noted.

---

[31] Testimony of the Wackenhut Corporation, *Private Investigative Firms*, Hearings before the Privacy Protection Study Commission, January 26, 1977, p. 213. (Hereinafter cited as "Private Investigative Hearings").

[32] Testimony of the Wackenhut Corporation, Private Investigative Hearings, January 26, 1977, p. 40.

[33] Credit Reporting Hearings, August 3, 1976, p. 247.

CamScanner

Types and Methods of Information Collection

Although preemployment reports emphasize past employment experience more than an insurance inspection report does, they lay stress on the same categories of "adverse" or "derogatory" information. Private investigative firms seek information on drinking habits, associates, drug use, personal habits, possible criminal behavior, personal reputation, and other items that might not show up in the records of a previous employer, or be volunteered by an applicant. Pinkerton's, Inc. testified that in a neighborhood check, they examine "primarily reputation and character." "We would even describe a house," said one witness, "whether it is well maintained, the grass is cut, depending upon the type of position."[34] Although they said they would not ask specific questions about sexual activities or preference, Pinkerton witnesses also said they would specifically inquire about current and past drug use and alcohol consumption.[35]

In its operations manual, one major private investigative firm directs its investigators to keep the following "basic and fundamental" points of inquiry in mind at all times:

(1) Character - general traits; reputation as to sobriety; honesty; trustworthiness; reliability; discretion; or lack of such qualities.
(2) Associations - types of persons, groups, or organizations, or movements with which person has been affiliated, with particular concern as to whether his associations have been undesirable in any way.
(3) Qualifications and ability - specific inquiry concerning qualifications and ability is essential.[36]

Beside compiling information through interviews, private investigative agencies also make inquiries of other record keepers. Included in one private investigative firm's list of "general sources of information" are the following: banks; collection agencies; small loan companies; savings and loan associations; land title companies; Federal narcotic agencies; postal authorities; the Internal Revenue Service; the Immigration and Naturalization Service; the Securities and Exchange Commission; the Department of Justice; the Department of Health, Education, and Welfare; State Comptrollers and tax offices; local school authorities; universities and other education facilities; and probation officers.[37] Although access to some of these records must be conditional upon obtaining the written authorization of the subject of the investigation, this is not explicitly provided for in the firm's manual. Moreover, it is widely alleged that because of the previous

[34] Testimony of Pinkerton's, Inc., Private Investigative Hearings, January 26, 1977, p. 157.
[35] *Ibid.*
[36] Until recently, investigators were also instructed to examine "loyalty," which was defined as, "actions or statements reflecting person's loyalty to employer; also, attitude and allegiance to the United States." The identity of this private investigative firm has been kept confidential at its request.
[37] The identity of this private investigative firm has been kept confidential at its request.

CamScanner

government employment of so many of their investigators, private investigative agencies are able to circumvent established authorization procedures.

The best example of this is the access which they are generally assumed to have to the centralized criminal history files maintained by State and local criminal justice agencies. The three private investigative firms which testified before the Commission all asserted that they have access to such files only where the law permits. However, Sorrell Wildhorn, a Rand Corporation analyst who has conducted the most far-reaching independent study of private investigative agencies to date, told the Commission that many private security executives freely admit to having access to " . . . the records of public law enforcement agencies . . . in jurisdictions in which policy or statutes prohibit such access."[38] It is said that to keep an employer from knowing about such practices, investigators commonly report the criminal history information as though it had been obtained from a police blotter or court records.[39]

Finally, the Wackenhut Corporation told the Commission that it used to maintain extensive files at its Coral Gables, Florida, headquarters on possibly "subversive" political activity, and other related information, and that these files were checked in the course of all background investigations, including preemployment investigations. The files, which Wackenhut no longer holds but to which its investigators still have access, were based on a collection of information, known as the "Barz Lag List," which Wackenhut purchased in February, 1966. Barz Lag, a retired naval officer, had monitored House of Representatives Internal Security Committee hearings and similar proceedings to sort out "derogatory-type" information on individuals for black-listing purposes.[40] Wackenhut purchased the Barz Lag material partly at the urging of some of its employer clients and partly out of its own desire to corner the private-sector market for such information. Subsequently, Wackenhut supplemented the Barz Lag files through an extensive newspaper clipping and general information-gathering program. Local offices, including the Washington, D.C., branch, were instructed to clip newspaper reports of political demonstrations or unrest—such as the civil rights and anti-Vietnam war protests of the late 1960's—as well as other events which might be of future interest. Patterned after the central files of the FBI, the information was indexed by individual and by subject, allowing a quick central-file check in the course of each background investigation the firm conducted. For a time, this file capacity was considered a major asset in marketing Wackenhut investigative services. However, when few employers expressed interest in it, Wackenhut donated it to the Church League of America, a political group which claims to hold "the largest and most comprehensive files on subversive activity, with the single exception of the FBI."[41] Today Wackenhut continues to use the Church League files when there seems to be a need to do so, but they are apparently not much in

[38] Private Investigative Hearings, p. 237.

[39] *Ibid.*

[40] Testimony of the Wackenhut Corporation, Private Investigative Hearings, January 26, 1977, pp. 44, 63-89.

[41] The Church League of America, *What is the Church League of America?* undated, p. 4.

CamScanner

demand. Pinkerton's and Per-Mar both testified that they have never maintained files of this nature, nor have their preemployment background reports ever contained information on political activities.[42]

Apparently employers, unlike insurers and credit grantors, are not much interested in sharing information about applicants and their backgrounds. This was demonstrated by a Wackenhut witness who testified that Wackenhut once considered establishing a central databank that employers could use to check out applicants and current employees:

> . . . we felt that there was a need on the part of business and industry to have a central index where they could secure information regarding the background of the individuals involved in various types of criminal as well as subversive activities; and we at one time contemplated setting up a procedure whereby, for example, we might accumulate information on individuals who are employed in the retail field, or people employed in the transportation industries, and provide a central index of information regarding those persons.[43]

The plan was abandoned, however, for lack of employer interest. The employers contacted were neither prepared to contribute information to the databank nor to pay for the service it would make possible. Apparently, the employer's desire for a high-quality, thorough, investigation, tailored to its specific needs, is a real one; and high-quality investigations cannot be reliant on a central databank. Moreover, there are more employers than insurers, and thus a much less concentrated demand for reports on applicants. Indeed, Wackenhut, the nation's third largest private security firm, testified that it currently maintains only about 70,000 files containing information on subjects of investigations done for clients.[44] Pinkerton's, Inc., the country's oldest and largest security firm, and Per-Mar Security, a much smaller firm, both testified that they do not centrally index reports done by local branch offices, nor do they retain investigative reports very long.[45] In fact, Pinkerton's testified that unless a preemployment report is needed for litigation or possible prosecution, it is destroyed as soon as the client pays the bill.[46]

On the other hand, private investigators doing preemployment work do have access to the information reservoirs maintained by the support organizations that service insurers and credit grantors. Employers, like insurers, view an individual's credit history as an important indicator of trustworthiness and responsibility; and credit bureaus, as a rule, have not

---

[42] Testimony of Pinkerton's, Inc., Private Investigative Hearings, January 26, 1977, p. 147; and testimony of Per-Mar Security, Inc., Private Investigative Hearings, January 26, 1977, p. 196.

[43] Testimony of the Wackenhut Corporation, Private Investigative Hearings, January 26, 1977, p. 43.

[44] *Ibid.*, p. 24.

[45] Testimony of Pinkerton's, Inc., Private Investigative Hearings, January 26, 1977, p. 144; and testimony of Per-Mar Security, Inc., Private Investigative Hearings, January 26, 1977, p. 191.

[46] Testimony of Pinkerton's, Inc., Private Investigative Hearings, January 26, 1977, p. 144.

CamScanner

been reluctant to share information in their records with insurers and employers who are willing to pay for it. Hence, private investigators and inspection bureau representatives both rely on credit-bureau records in writing their reports, and as leads to further sources of investigation.

Moreover, for some reason, private investigative agencies will not identify a credit bureau as the source of information in a preemployment report. One major firm's investigative manual says that:

> Information obtained from Dun and Bradstreet and from various credit bureaus should be treated as coming from a confidential source and should not be reported in the language of the credit agency. This information should be reported in the language of the investigator, disguising its origin.[47]

One consequence of this, of course, is to make it impossible for either the employer or the applicant to trace an error back to its source.

There is also some evidence that private investigative agencies have access to inspection bureau files. A senior employee of one of the larger investigative agencies told the Commission staff that it is not uncommon for an investigator to establish a "source" relationship with an inspection bureau, but again always disguising the source.

Investigative Services in Adversary Situations

In addition to conducting underwriting and preemployment investigations, inspection bureaus and private investigative agencies both provide special investigative services to assist insurers in the settlement of certain types of claims. Private investigative agencies may also offer extensive "loss prevention" services to employers. In both instances, experienced and highly trained investigators are assigned to the case; and in some cases mechanical surveillance devices may be used.

Transfer to the "special investigations" claims unit is considered a promotion for the inspection bureau field representative, and the reports they prepare are carefully checked before they are delivered. Claims settlement and loss prevention investigations are adversary situations which may lead directly to a court room, so the evidence standards of both client and investigator are high. Moreover, the potential savings to the insurance company or employer are great. Fraud is estimated to be involved in hundreds of millions of dollars worth of insurance claims each year. While even the most complete investigation rarely results in a prosecution for criminal fraud, a good investigation can frequently force a fraudulent claim to be dropped or produce a much-reduced settlement. Similarly, it is estimated that well over three-fourths of all business inventory shortages are the result of theft by employees. Theft from retail establishments alone amounted to an estimated $7.2 billion in 1976.[48] Thus, even a very expensive investigation can turn out to be cost-effective.

Where large amounts of money are at stake, investigators may use

[47] The identity of this private investigative firm has been kept confidential at its request.
[48] U.S. Department of Commerce, *Cost of Crimes Against Business*, O.B.R.A., 1976.

unusual techniques. In a personal injury case, standard investigative practice is to conduct an "activities check," which may involve covert surveillance of the individual, possibly photographic surveillance. Along these lines, investigators working for a company with theft or other problems may place an "intelligence agent" undercover in the company's work force to observe the activities of other employees. Whether or not this produces direct results, the sense that it may be going on can have a desirable inhibiting effect.

Pretext interviews in claims investigations are another routine practice. Wackenhut witnesses described how one such interview might be conducted:

> Well you might, for example, call up and ask the lady of the house, who apparently is the claimant in connection with the matter, what type of detergent or soap she might use in laundering her wash, and she would tell you. And you would indicate to her without even disclosing what company you are with and who you represent that you would like to come out on Monday morning or whenever she does her washing in order to take some pictures of her using that product. And, then you would appear on the scene and she would wash. And, you would have a person who has a serious back injury who is claiming a large amount of money from the insurance company, who proceeds to wash and hang up her wash on the washing line. That might be one example.[49]

Because of the importance of medical-record information in claims settlments, Equifax Services Claims Department maintains special card files on "medical sources." A source card generally indicates the most opportune times for obtaining information from the doctor, whether an authorization is commonly required, the doctor's attitude toward insurance companies, and so forth.[50] Of the 11,000 hospitals accredited in the United States and Canada, Equifax estimates that its agents are able to make a personal review of the records in all but 1,200, the 1,200 being known in the business as "problem hospitals."[51]

An extreme example of the use of pretexts to gain access to medical records without authorization was provided in testimony by the Denver, Colorado, District Attorney during the Commission's Medical Records Hearings in Los Angeles.[52] Factual Service Bureau, Inc., (FSB) a private investigative agency headquartered in Chicago but with offices scattered around the country, was said to have made the unauthorized acquisition of medical-record information for use in investigating and settling third-parties insurance claims its "bread and butter" business. According to the evidence presented to the Commission, this was apparently done by phoning a hospital records room, pretending to be a doctor, or by paying a strategically

[49] Private Investigative Hearings, January 26, 1977, p. 54.
[50] Equifax, Inc., "Claim Reports Manual," November 1975, p. B-3.
[51] *Ibid.*, p. C-11.
[52] Testimony of Dale Tooley, *Medical Records*, Hearings before the Privacy Protection Study Commission, June 11, 1976.

CamScanner

placed hospital employee to spirit the records out. FSB also claimed to be able to acquire records from the "IRS and financial sources," creating the impression that it could penetrate both.

Although aspects of Factual Service Bureau's *modus operandi* are described in several parts of this report, two points are important here. First, while the Commission realizes that the type of practices in which Factual Service Bureau engaged are rarely, if ever, used in underwriting or preemployment background investigations, and further that they are not typical even in most claims investigations, the fact that there was any kind of market for such a service should be a matter of great concern. Second, it must be understood that the reports Factual Service Bureau prepared were not subject to any of the requirements of the FCRA by virtue of the fact that they were developed in connection with claims investigations which the Act does not reach.

COMPLIANCE WITH THE FAIR CREDIT REPORTING ACT

At the time it was enacted, the primary objective of the FCRA was to improve the accuracy, timeliness, and completeness of the information credit bureaus, inspection bureaus, and private investigative firms report to their clients. To this end the Act made it possible for the subject of an investigation to review and challenge information in the report that results from the investigation. Implementation of these provisions, however, has not been without its problems; and the Act today remains a much less effective protection for the individual consumer than he needs. The reasons why this is so in the credit area are explained in detail in Chapter 2, and the chapters on insurance and employment record keeping (Chapters 5 and 6) highlight similar problems in those areas.

Based upon the testimony it has taken and the analysis of the extent to which the FCRA comports with the Commission's three recommended policy objectives regarding intrusiveness, fairness, and expectation of confidentiality, the Commission has concluded that additional legislative action is clearly needed. While the practices of investigative-reporting agencies have certainly changed significantly over the past six years, and although it appears that the practices of some inspection bureaus and private investigative firms now meet not only the objectives of the Act but also the objectives of the Commission's recommendations, this is not universally so, nor has the process by which it has sometimes come about been a reassuring one.

This is sharply illustrated by the experiences of one Commission witness who sought to challenge the information in an inspection bureau report which prompted cancellation of his auto insurance.

The Millstone Case

In August 1971, journalist James C. Millstone moved from Washington, D.C. to St. Louis, Missouri, to assume the post of news editor for the *St. Louis Post Dispatch.* He asked his insurance agent to place automobile

insurance for him. A policy with Firemen's Fund took effect on November 15. A few days later, Millstone received a form notice that a personal investigation would be made in connection with the new policy. On December 20, Firemen's Fund informed Millstone's agent that the policy would be canceled as a result of information turned up in an inspection report prepared by O'Hanlon Reports, Inc.

Because the agent was willing to vouch for him, and because of Millstone's standing in the community, Firemen's Fund was shortly thereafter persuaded to ignore the report and reinstate Millstone's policy. However, getting the report itself cleaned up was not so easy. On December 22, 1971, Millstone went to the St. Louis office of O'Hanlon Reports. The office manager told him that he was entitled to know what was in his own report, but that O'Hanlon was by law allowed 10 days to produce the information. When Millstone protested, the manager called O'Hanlon's New York Headquarters and let Millstone speak to one Kenneth Mitchell. Mitchell told Millstone that the file was in the mail from St. Louis to New York and would be made available as soon as possible. As it later came out in court, however, Millstone's file was actually in the St. Louis office when he visited it and was only mailed to New York after he left.

Six days later, when Millstone returned to the St. Louis office, the manager read from a single sheet the purported contents of Millstone's file. The disclosure sheet, prepared by David K. Slayback, Vice President of O'Hanlon, said in part:

> The file shows that you are very much disliked by your neighbors at that location [Millstone's Washington residence] and were considered to be a "hippy type." The file indicates that you participated in many demonstrations in Washington, D.C., and that you also housed out-of-town demonstrators during demonstrations. The file indicates that these demonstrators slept on floors, in the basement, and wherever else there was room on your property. The file shows that you were strongly suspected of being a drug user by neighbors, but they could not positively substantiate these suspicions. You are shown to have had shoulder-length hair and a beard on one occasion while living in Washington, D.C. The file indicates that there were rumors in the neighborhood from three previous residences in Washington, D.C. prior to living at the 48th Street, N.W. location.[53]

This disclosure was read to but not shown or given to Millstone for his own examination.

Shocked, Millstone disputed virtually all of the information disclosed to him and demanded an explanation of several of the allegations. The office manager told Millstone he had no further information and could not answer Millstone's questions. He said that his instructions from the New York office were to read the disclosure sheet and note any item disputed by Millstone. The actual report from which the disclosure was abstracted was

[53] *Millstone v. O'Hanlon Reports, Inc.*, 383 F. Supp. 269, 271 (1974).

neither produced nor quoted. The manager, however, called New York once again; and this time Millstone spoke to David Slayback. Slayback defended the method and propriety of the disclosure process and refused to expand on the statement that Millstone was strongly suspected of being a "drug user."

Slayback directed the manager of O'Hanlon's Silver Spring, Maryland, office, which had conducted the original investigation, to reinvestigate. The Silver Spring office took approximately three days to do so and report back to New York. A further abstract was prepared. The abstract based on the reinvestigation contained new charges and led to another series of meetings and telephone calls between O'Hanlon representatives and Millstone. In each conversation and meeting, Millstone asked to see his file but was refused.

Eventually, Millstone sued O'Hanlon. During the pre-trial discovery process, Millstone learned about critical comments concerning his wife contained in his file, but never previously disclosed to him, as well as additional derogatory allegations about himself.

One of the documents Millstone introduced as evidence at the trial was the handbook O'Hanlon issued to each branch office manager. The manual states in part:

> The important thing is to NEVER check the files in the presence of the consumer . . . prior to the time of your appointment with the consumer, you will have received the Statement of Disclosure from the Home Office. At the time of your appointment ANY and ALL information you may have relating to the consumer, such as copies of files, a copy of your statement, index cards, etc., are to be in your desk drawer out of SIGHT of the consumer. You are not to show anything or acknowledge that you have anything other than the Statement of Disclosure.
>
> Actual disclosure will be accomplished by reading the Statement of Disclosure to the consumer. The Statement is to be read word for word at your normal reading speed. It is not to be read slow enough for anyone to copy down word for word, nor is it to be read so fast that the consumer will not understand what you were saying. Part or all of the Statement of Disclosure may be reread if the consumer indicates he did not understand what you were telling him. The consumer and/or the person with him may not have a copy of the Statement, nor may they be allowed to read the Statement or touch it.[54]

It was disclosed that an O'Hanlon employee, Alexander Mayes, conducted the original investigation of Millstone. Mayes claimed to have spoken to four former neighbors of the Millstones on the block where they had lived in Washington, D.C. Of the four, one refused to speak to Mayes and two told him that they knew of trouble in the neighborhood but that they knew nothing firsthand and that they did not wish to be involved. All of the data in the Mayes report were purported to have come from one

[54] *Ibid.*, 272, 273.

neighbor, "McMillan," who was deceased at the time of the Millstone suit. Mayes averaged approximately 70 to 80 reports a week and spent from 10 to 30 minutes on each insurance investigation.

Millstone's character, reputation in the community, working and personal habits, and his family relationships were testified to by character witnesses of national reputation at the trial. These witnesses were entirely supportive of Mr. Millstone and contradicted the O'Hanlon report allegations totally.

The court found that Mayes had "knowingly included false information in the report," and further that O'Hanlon's,

> methods of reporting on consumers' credit backgrounds as shown at the trial were so slipshod and slovenly as to not even approach the realm of reasonable standards of care imposed by the statute [FCRA].[55]

Millstone was granted $2,500 in actual damages, $25,000 in punitive damages, and $14,000 in attorney's fees. The decision was appealed by O'Hanlon, but finally upheld in January 1976.[56]

While Mr. Millstone's experience by no means typifies the treatment of all or even a sizeable minority of the individuals investigated by inspection bureaus and private investigative agencies, it shows why the FCRA needs to be strengthened substantially. Only a small percentage of inaccurate information reports result in litigation, and many cases that go to court are settled before judgment. The Millstone case was filed in April 1972, within months after the Act took effect, and has established legal precedents of wide-reaching effect. Yet the case was not settled until the U.S. Court of Appeals rendered a decision four years later. Meanwhile, the inspection bureau vigorously fought each step of the way and apologized to Mr. Millstone only in August 1976 during its testimony before the Privacy Protection Study Commission.

Many consumers are still not aware that legal recourse is available to them and many who are will nonetheless try to cope with the damage done rather than bring suit. Litigation is expensive, uncertain, protracted, and possibly demeaning as one attempts to document one's own reputation. Further, as the *Millstone* case illustrates, some inspection bureaus, in complying with the access and dispute requirements of the FCRA first developed policies which discouraged all but the most persistent, and which had the effect of obscuring the actual content and sources of information in a report unless the aggrieved individual was willing to go to court. Only recently did they start allowing an individual to see and copy a corrected inspection report upon request, and some still do not allow the individual to do even that.

THE COMMISSION'S RECOMMENDATIONS

The activities of the investigative support organizations described in

[55] *Ibid.*, 275.
[56] 528 F.2d. 829 (8th Cir., 1976).

this chapter present a number of special privacy protection problems. In part because of the broadly worded authorization forms that applicants for insurance and employment are often asked to sign, the crucial role these organizations can play in the decision-making processes of insurers and employers is poorly understood by the public. As indicated in the chapters on the insurance and employment relationships, blanket, open-ended permissions for unnamed third parties to make almost any kind of inquiry about an individual tend to obscure the fact that an inspection bureau or private investigator, rather than the insurer or employer, may actually do the information gathering and perhaps retain the results for subsequent reporting to others. Moreover, the information gathered and reported may often disguise its source, thereby making it impossible to tell whether an individual's presumed confidential relationship with a record-keeping institution, such as a credit grantor, an insurer, a medical-care provider, or his employer, is, in fact, being honored.

Furthermore, in the insurance area, the economic incentive to assure that the information in an inspection report is accurate, timely, and complete has traditionally been weak. Although inaccurate or false information can lead a company to turn down an applicant who would otherwise qualify for average or even preferred rates, it takes a large number of policies lost as a result of inaccurate inspection reports to more than make up for a $50,000 claim settlement that might have been avoided if information developed by an inspection bureau report had been used as the basis for declining or refusing to renew. Clearly a service which will help a company avoid even a few substantial claims or which tends to raise premium income even a small amount is quite valuable. Indeed, it can make a great deal of difference to an insurer in terms of earnings and competitive position, thereby directing attention away from the fact that it can also be a cause of considerable unfairness to some unknown number of individuals whose reports contain inaccurate information.

Finally, to the extent that inspection bureaus rely on information in their own files in making reports, they can play a gatekeeping role that significantly affects an individual's ability to establish relationships with a large number and variety of record-keeping institutions. Where adverse information is kept on file for many years, an individual may never be able to avoid having certain lines of inquiry made about him, and thus never be able to escape the subjective judgments of others as to whether he still has the questionable characteristics that were once reported about him. While this may not have the same "chilling effect" on an individual as government inquiries about aspects of an individual's private life are reputed to have, it presents at least the danger of permanent, inescapable stigmatization.

In recognition of these problems, the Commission has made recommendations regarding the insurance and employment relationships which, if adopted, will markedly alter the role that investigative support organizations play in them. The recommendations would redistribute responsibility for the practices of inspection bureaus and private investigative agencies by requiring their users to exercise reasonable care in selecting and evaluating them, and, in addition, levy access and correction requirements on users

CamScanner

which parallel those that would apply to report preparers. Equally important, the Commission's recommendations would enlarge the population of individuals entitled to the protections afforded by the FCRA, change the Act's access and correction requirements to make them better serve the interests of the individual, and regulate, to some degree, the investigative techniques that may be used by insurers, employers, and investigative support organizations that serve them.

Redistribution of Responsibility

The Fair Credit Reporting Act establishes liability for the accuracy, timeliness, and completeness of investigative reports, but currently places it exclusively on the inspection bureaus and investigative agencies that prepare them. The user of a report bears no responsibility for the conduct of the investigative support organization that put the report together, nor is it under any obligation to inform the support organization when it discovers an error. Indeed, the likelihood that it will discover an error is low, since the FCRA only allows an individual to check and, if necessary, correct the copy of an investigative report that the support organization retains. The Act gives him no parallel right with respect to the same report in the hands of the insurer or employer user. The user's responsibility is limited to notifying the individual that a report may be requested, describing, upon request, the scope of the investigation, and, if an adverse decision results, notifying the individual of the name and address of the inspection bureau or private investigative agency that prepared the report.

The Commission's solution to this problem is to place the insurer and employer in a position of joint responsibility with the investigative support organization. While accountability for the contents of a report would remain with the organization that prepares it, the user would be liable if it repeatedly did business with any support organization that consistently engaged in objectionable practices. Moreover, by requiring the user, as well as the preparer of a report, to disclose its contents to the individual whom it concerns and to cope with certain types of deficiencies in it that the individual may allege, the user is given a strong incentive to deal only with support organizations that produce reports of high quality.

Some investigative support organizations currently have contracts with their users that make the user who discloses the contents of a report to its subject the liable party in any law suit that may result. The effect, of course, is to keep the user from disclosing anything to the individual, and the Commission's recommendation would therefore make such contracts null and void. Finally, the Commission's "expectation of confidentiality" recommendations and proposed authorization requirements are worded in such a way as to compel support organizations to live by the same ground rules on third-party access to reports as the insurers and employers who use them. In practical terms, this means that a report prepared on an individual for one purpose will no longer be useable for another purpose without his authorization, thereby giving him some control over the circulation of

information about him which has been generated in service of markedly different record-keeping relationships he maintains or seeks to establish.

Scope of the FCRA

A second shortcoming of the FCRA is that its protections do not reach every individual who is the subject of an underwriting or preemployment investigation—notably any individual whom an insurer or employer investigates on its own or who is investigated in connection with a job for which he has not applied. The Commission has heard of no plausible rationale for preserving such a distinction and thus, through judicious wording of its various recommendations affecting the FCRA, has eliminated it.

Access and Correction Requirements

Perhaps the most blatant weakness in the FCRA is the impracticality of its provisions aimed at giving an individual a way of getting inaccurate, incomplete, or obsolete information in an investigative report corrected, amended, or deleted. As was evident in the *Millstone* case, requiring only that the "nature and substance" of a report be revealed to the individual effectively deprives him of his corresponding right to challenge its content. Thus, in its insurance and employment recommendations, the Commission proposes that the FCRA be amended to allow an individual to "see and copy" a report about himself, whether in the hands of the preparer or the user and regardless of whether they happen to be the same organization (as when an insurer or employer conducts its own investigation of an individual). In conjunction with this change in the Act, the Commission also recommends that the individual be able to receive a copy of a report in the mail, and, for reasons discussed in the chapter on the employment relationship, that an employer automatically send an applicant or employee a copy of any background report prepared on him. (Note that the Commission's recommendation on applicant interviews in the course of preparing underwriting reports could also be satisfied by mailing the applicant a copy of the report.)

Of equal importance is the corollary obligation the Commission's recommendations would place on an insurer or employer to propagate corrections, amendments, disputes, and deletions of information in a report back to the support organization from whence the information came. So, also, the Commission's recommendations that would prohibit the use of information concerning previous adverse insurance decisions, and the disclosure by insurance institutions and support organizations of information concerning an individual's health which has not been obtained from a medical-care provider or from the individual himself, or from his spouse, parent, or guardian, should serve to reduce the amount of damaging gossip in inspection bureau reports.

CamScanner

Investigative Techniques

Finally, the Commission has recommended Federal legislation that would (1) outlaw the use of pretext interviews in all insurance (including claims) and preemployment investigations; (2) prohibit an employer from using polygraph or other truth verification equipment to gather information from an applicant or employee; and (3) make it a criminal offense to seek to acquire medical-record information from a medical-care provider through false or misleading representations.

AN AGENDA FOR FURTHER STUDY

If accepted, the Commission's recommendations should go a long way towards improving the practices of inspection bureaus and private investigative agencies. There are, however, a number of problem areas that deserve further study.

In the employment area, particularly, further study is needed of the access which private investigators are alleged to have to computerized criminal histories maintained by public law enforcement agencies. If there is indeed a "buddy system" which facilitates unauthorized access to such records, it should be exposed and dealt with responsibly. Additional examination is also needed to assure that "blacklists" and reports concerning an individual's political beliefs and associations are not being used in making employment decisions. In this regard, the activities of organizations like the Church League of America need to be studied further.

The loss prevention services and background investigations for parties other than employers which many private investigative agencies offer their clients are still another category of activities that merits examination. The Commission has not been able to look at possible uses of private investigators to monitor union activity or the activities of individuals whose political views conflict with those of their employer or of any other investigative agency client. Finally, the effectiveness of requiring a private investigator to have a signed authorization in hand before he can acquire information in records maintained by an institution with whom an individual has a legally enforceable confidential relationship will be a crucial question for the future.

Adoption of the Commission's recommendations regarding investigative reporting agencies will involve some sweeping changes in current practice. The record of the last 10 years does not suggest that those changes will be easily wrought. Hence, in recognition of the impact that investigative-reporting activities can have on the lives of many individuals, the Commission believes that continued monitoring is not only advisable; it is essential.

CamScanner

Chapter 9

Government Access to Personal Records and "Private Papers"

Discussion of the need to protect individuals from threats to personal privacy often conjures up ominous images of government agents conducting surreptitious investigations and compiling dossiers. Such images come forcefully to mind when one is concerned, as the Commission is, with preventing improper inquiry into and disclosure of records about individuals. While the tendency to equate threats to personal privacy with government action, and government action with clandestine police operations, is understandable, the evidence uncovered in the Commission's inquiry shows that such equations are not necessarily accurate.

The improper collection and use of information about an individual present as difficult problems when private institutions fail to observe the legitimate rights and expectations of the individual as when government fails; but, governmental intrusions on personal privacy have a longer and more dramatic history, both in law and in the public mind. Generous portions of the Bill of Rights were fashioned two centuries ago to assure that Americans would not again suffer the unwarranted intrusions by government which, in John Adams' mind, provided the spark that ignited revolution.[1] Protection from government intrusion, as exemplified in the Fourth and Fifth Amendments, has long been the primary public focus of privacy protection.[2] The desire to assure for the individual the quiet enjoyment of his home in part justifies such protection; but in equal part, individual rights securing privacy are also intended to safeguard the personal papers and other documentation that can illuminate the associations, interests, attitudes, and beliefs as well as actions of an individual.[3] Such information is valuable in a variety of forms of government coercion, ranging from criminal prosecution to less legitimate activities. Indeed, this second aspect of personal privacy is the focus of Fourth Amendment protection, the "search and seizure" standards which never fail to stir public

---

[1] Hiller Zobel and Kinvin Wroth (eds.), *Legal Papers of John Adams*, (Harvard University Press, Cambridge: 1965) Vol. 2, Case No. 44, pp. 106-144.

[2] John Eger, "Foreward" to Kent Greenawalt, *Legal Protections of Privacy*, Office of Telecommunications Policy (Washington, D.C.: 1976); Thomas I. Emerson, *The System of Freedom of Expression*, (New York: Vintage, 1970) pp. 544-48.

[3] See Note, "Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments," 90 *Harv. L. Rev.* 945 (1977) (hereinafter cited as 'Formalism, Legal Realism . . . .").

CamScanner

interest and win extensive press coverage when debated in the Supreme Court.

These well publicized elements of Constitutional controversy and national history, perhaps inevitably, tend to focus on problems of law enforcement officers improperly gaining access to one's home or one's private records. Along with this emphasis on invasions of privacy by law enforcement comes a tendency to treat the issues as legal issues rather than policy ones, because, after all, the battleground for resolving those issues has traditionally been the courts. Earlier chapters of this report should dispel the impression that dangers to personal privacy are only products of government action, but the equation of government action with law enforcement activity needs to be tempered and the notion needs to be dispelled that resolving the basic privacy issues raised by government action demands a close attention to legal niceties.

The question of law enforcement, and the peculiar powers and opportunities to acquire information given government for that purpose, raise uniquely sensitive problems. Nonetheless, government's expanding role as regulator and distributor of largess gives it new ways to intrude, creating new privacy protection problems. By opening more avenues for collecting information and more decision-making forums in which it can employ that information, government has enormously broadened its opportunities to embarrass, harass, and injure the individual. These new avenues (and needs) for collecting information, particularly when coupled with applications of modern information technologies, multiply the dangers of official abuse against which the Constitution seeks to protect.[4] Recent history reminds us that these are real, not mythical, dangers.

The concern about governmental abuse which underlies traditional protections against government intrusion on personal privacy provides a focal point for exploring the particular balancing of interests which faced the Commission in reaching its recommendations on government access to private records as well as for emphasizing the need *not* to confine such deliberations within the narrow precincts of law. Though solutions must finally be fashioned into law, the choices made in arriving at such solutions are not mere legal choices; they are fundamental public-policy decisions—social and political value choices of the most basic kind.

The balance to be struck is an old one; it reflects the tension between individual liberty and social order. The sovereign needs information to maintain order; the individual needs to be able to protect his independence and autonomy should the sovereign overreach. The peculiarly American notions of legally limited government and the protections in the Bill of Rights provide broad theoretical standards for reaching a workable balance. But the world has a way of disrupting the particular balance struck in past generations; the theory may remain unaltered but circumstances change, requiring a reworking of the mechanisms which maintained the balance in the past.

---

[4] *Infra*, this Chapter, "Restricting Compulsory Reporting Requirements;" also, Chapter 13.

CamScanner

Current threats to personal privacy stem largely from changes in the way individuals go about their day-to-day business.[5] The Commission's inquiry did discover, however, that some threats are the result of government rewriting the rules of the game without letting the rest of the players know.[6] Both circumstances combine to erode the effectiveness of traditional protections for personal privacy and individual liberty.

Traditionally, the records an individual might keep on his daily activities, financial transactions, or net worth were beyond government reach unless the government could establish probable cause to believe a crime had been committed. If government were merely suspicious and wanted to investigate, such records were unavailable. The legal standards that protected them evolved in a world where such records were almost universally in the actual possession of the individual. Reflecting that reality, the law only barred government from seizing records in the possession of the individual.[7] As the record compiled by the Commission proves, that world no longer exists. Third parties, institutions or persons other than the individual, now keep a great many records documenting various activities of a particular individual. Indeed, these third parties keep records about the individual he would not ordinarily have kept in the past. Records for life and health insurance, for example, are repositories of highly intimate personal data, financial and familial as well as medical, which were virtually unknown until recent decades.

Financial records, particularly the information retained in demand deposit accounts, provide another instance where the changing patterns of life took the possession of information about himself out of the control of the individual. Of great importance, checking account records present a situation where alterations in record-keeping patterns have been exacerbated by government action. Until recently the account record maintained by one's bank frequently did not include a copy of each individual check, with the payee, date, and often place and reason for drawing the check clearly noted; rather, the record might simply have noted the dollar amounts of transactions and the date of processing by the bank.[8] The Bank Secrecy Act of 1970 and the Treasury regulations which give that law effect, however, now *require* depository institutions to keep copies of the checks an individual uses to draw on the funds in his account.[9] The checking account

---

[5] See, e.g., Chapter 2, "Consumer-Credit Relationship."

[6] *Infra*, this Chapter, "The Grand Jury Subpoena."

[7] *Boyd v. United States*, 116 U.S. 616 (1886); *Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting); *infra*, this Chapter, note 81.

[8] As Representative Patman explained during the debates preceding passage of the Bank Secrecy Act, a primary purpose of the Act was to "make uniform and *adequate* the present record-keeping practices, or *lack of record-keeping practices*, by domestic banks and other financial institutions," (emphasis added) 116 *Cong. Rec.* 16951 (1970); also, see remarks of Representative Stark, *Administrative Summons and Antidisclosure Provisions of the Tax Reform Act of 1976*, Hearings before the Subcommittee on Oversight of the Committee on Ways and Means, U.S. House of Representatives, 95th Congress, 1st Session, ser. 95-4, at 26 (February 24, 1977) (hereinafter cited as "U.S. House of Representatives, Hearings on Administrative Summons").

[9] 12 U.S.C. 1951 *et seq.*; 31 C.F.R. 103.

CamScanner

has become an intimate mirror of individual activity in a way it never was before the Bank Secrecy Act.

The existence of records about an individual that are not in his possession poses serious privacy protection problems, especially when government seeks access to those records. Record keepers can, often do, and sometimes must, disclose records about an individual to government without seeking the individual's approval, whether the disclosure is at the request of government or through the initiative of the record keeper; and, frequently no record of the disclosure is ever made. A government request made informally through a personal visit to the record keeper or by a telephone call, for example, may leave no trace in any record. The individual may never know that agents of the government have inspected his records. Except in a limited number of situations, neither the record keeper nor the government is obliged to notify him that his records were opened to government scrutiny. Even if the individual is given notice and documentation of the disclosure, he has no legal right to challenge the propriety of government access to his records, despite the possibility that the government agent might have been on a "fishing expedition."[10]

Historically, the courts have justified relatively unrestricted government access to records on individual activity kept by third parties by regarding such information as independent documentation of voluntary transactions between the individual and the record keeper.[11] Coupled with this concept of voluntariness, such records have not been viewed, and until recently rightly so, as the sorts of private records and personal papers that merit special protection because they illuminate an individual's associations, interest, attitudes, and beliefs, as well as actions. The privacy protections that help secure the independence and autonomy of the individual were not considered necessary. Courts and the public were comfortable with a legal standard that protected only records in the possession of the individual.

Today, the law remains unchanged even though new sorts of personal records, created to meet new circumstances, sometimes generated by government requirements, are vulnerable to seizure or inspection by government without the individual being able to intervene. A record keeper may volunteer information about an individual to government; or the Executive branch of government can compel production of such records with little trouble and often without supervision by the judiciary or anyone else.[12] Recently, the courts have begun to doubt the assumptions of voluntariness upon which they rest their refusal to extend basic constitutional protections to an individual when government seeks disclosure of records held by a third-party record keeper. Indeed, some judges have taken tentative notice of the realities of contemporary record keeping and the danger that allowing government to acquire such "third party" records

---

[10] See, e.g., *United States v. Miller*, 425 U.S. 435 (1976); *Kelley v. United States*, 536 F.2d 897 (9th Cir. 1976); compare, *Donaldson v. United States*, 400 U.S. 517 (1971); also, see *infra*, note 94.

[11] *Ibid.*

[12] *Infra*, this Chapter, "Regulating the Compelled Production of Records."

might disclose "intimate areas of personal affairs" protected by the Fourth and Fifth Amendments.[13]

Nonetheless, to wait on the courts to reweave the fabric of law and create protections for the individual is to adopt a policy of uncertain outcome. One cannot be sure the courts will become more flexible. One can be sure, however, that if the courts do extend protections, their efforts will be slow and piecemeal. Yet the society is faced with problems that demand decision and resolution. The world has altered and continues to change with increasing rapidity. As the Commission's study of Electronic Funds Transfer Systems suggests, existing problems with government access to records will be exacerbated by future developments; they will not go away.[14] Today, government has access to the most revealing personal records about an individual; yet the individual has no ability to thwart or even contest such access. Perhaps most important, they are situations in which the individual has no choice but to allow others to maintain records about him. Not to enter into the relationships that generate individually identifiable records would subject the vast majority of Americans to severe economic and social burdens, disrupting the ordinary course of their lives. Think, for instance, of the time and effort necessary to pay all bills in person, not to mention the risk involved in carrying enough cash to transact all personal business.

Further, and of increasing importance, there is little to impede government access to records about individuals held by third parties, particularly records the government requires third parties to keep. In its Depository and Lending Institution hearings, witnesses told the Commission that informal access to bank records, i.e., access without a subpoena or summons, was a favorite tool of government investigators. Indeed, the American Civil Liberties Union submitted testimony originally given before the House Judiciary Committee in July, 1975, which suggested that such informal or "voluntary" disclosure was "the means by which government normally procures access to confidential bank records."[15] The Internal Revenue Service testified that banks are usually cooperative in responding to a "friendly" summons.[16] Even when banks are somewhat less cooperative, however, little real impediment to government access occurs. Continental Illinois Bank, for example, seeks to notify the individual that his account records have been subpoenaed and does a "four corners" check of the validity of any summons received,[17] but, as explored below in more detail, neither action by the bank gives any real assistance to the individual. And,

---

[13] *California Bankers Assn. v. Schultz*, 416 U.S. 21, 78 (1975) (Powell, J., concurring).

[14] See Chapter 3, "The Depository Relationship," section on "Electronic Funds Transfer Services: An Overview."

[15] Written Statement of Hope Eastman, Associate Director, ACLU, *Depository and Lending Institutions*, Hearings before the Privacy Protection Study Commission, April 22, 1976, p. 5 (hereinafter cited as "Depository and Lending Institutions Hearings").

[16] Testimony of the Internal Revenue Service, Depository and Lending Institutions Hearings, April 22, 1976, pp. 777-830, and particularly pp. 804-07.

[17] Testimony of Continental Illinois Bank and Trust Company, Depository and Lending Institutions Hearings, April 21, 1976, p. 277.

CamScanner

the extent of concern exhibited by Continental Illinois for its customers is rare.

The Commission's hearings on the record-keeping practices of credit grantors and depository and lending institutions and its survey of credit-card issuers indicate that a large proportion of private-sector financial record keepers lack any policy on government access, not to mention a policy as fair as that of the Continental Illinois Bank.[18] In addition, what is labeled "policy" is frequently little more than a grant of discretion—to notify or not, to determine the validity of a subpoena or not—given to an office manager or perhaps someone lower in the heirarchy. Some record keepers even seem to have a policy of *not* notifying the individual or reviewing the validity of the subpoena. Such lack of policy, however, should not be viewed as unkindly as a first reaction might suggest. As American Express testified in February, 1976, it did not notify customers as a matter of course because it could not see what good it would do.[19] Though its position was not particularly well received by the public, American Express was right; notice to the customer does little good. Even if notified, the individual can do little to hinder government access, however illegitimate the purposes or improper the procedures.[20] The ground rules need to be changed if any good is to be done.

To effect that change successfully, a brief exploration of the arguments that have prevented the courts from extending constitutional protections for private papers to bank account and similar records will illuminate the range of policy decisions the Commission addressed and the basic choices that must be made.

THE LIMITS OF LEGAL PROTECTION: AN OVERVIEW

If records about individuals held by third-party record keepers are to be protected against government access, the law must change. In light of the inability of the courts to refashion the application of Constitutional theory, the change must come through legislative action.

Voluntary Disclosure and Compulsory Process

Government access to the account records of depository institutions provides an excellent example of the need for change and illustrates the importance of understanding current standards. In *United States v. Miller*,[21] the Supreme Court reaffirmed the traditional legal standard that customer account records in a bank are not the private papers of the customer. An

[18] See Chapter 2, "Consumer-Credit Relationship," section on 'Disclosures to Government Agencies", particularly the discussion of the credit-card issuers survey; also, generally, Depository and Lending Institutions Hearings, April 21-22, 1976.

[19] Testimony of American Express Company, *Credit-Card Issuers*, Hearings before the Privacy Protection Study Commission, February 11, 1976 (hereinafter cited as "Credit-Card Issuers Hearings").

[20] *Infra*, this Chapter, "Regulating the Compelled Production of Records"; "Formalism, Legal Realism . . . .," 90 *Harv. L. Rev.* 945, 964-85.

[21] 425 U.S. 435 (1976).

individual has neither ownership nor possession of such records, reasoned the Court; therefore, the records are simply the "business records of the bank." This line of argument and the precedents which have developed it extend back through the Eighteenth Century.[22] The crucial element in this traditional view is that the individual, lacking a "proprietary" interest in a bank's records of his account, has no legal right he can assert to challenge access to those records by government or anyone else.

In California, the legal status of bank account records has been altered. Interpreting a 1972 amendment to the State Constitution, the California Supreme Court ruled that "a depositor has a reasonable expectation [that] the information and documents he furnishes his bank in connection with his account will remain private."[23] Because of this legal expectation, the disclosure of bank records to government without "proper legal process" amounts to an illegal search and seizure under California law. Proper legal process, according to the developing judicial interpretation, means that the probable cause standard a search warrant must meet becomes the minimum standard government must establish when seeking to compel the production of bank records. Perhaps more important, government may not request and receive an individual's bank records from the bank without employing legal process, unless, of course, the individual consents.[24] Put simply, California law provides the individual with a "legitimate expectation of privacy," which gives him a protectible legal interest in his bank records and, given that interest, the legal tools to protect his records.

The contrast between the *Miller* decision and California law highlights two issues: (1) the question of "voluntary" disclosure of information by third-party record keepers, that is, the discretion to disclose to government without the compulsion of legal process; and (2) the necessity of a substantive standard an individual can assert to protect records about him.

However detailed and carefully structured limitations on compulsory disclosure to government may be, as long as government can request and receive information from records about an individual on an informal or voluntary basis, little real protection of personal privacy will be achieved. If a record keeper has the discretion to disclose voluntarily, it will be hard for record keepers, particularly in heavily regulated sectors such as banking, to resist pressures for "voluntary" compliance with government requests for information. Voluntary disclosure of information on individuals held by third parties must be limited if limitations on compelled disclosure are to mean anything.

Limiting voluntary disclosure involves two distinct, though related, steps. One is to require government agencies to use legal process to obtain records and to notify the individual that his records are being sought. This

---

[22] The lack of any assertable legal interest in bank notes themselves, not to mention records of banking transactions, except a limited protection against theft, is chronicled by Blackstone, *Commentaries*, Vol. 4, p. 234; also, *Ibid.*, Vol. 3, p. 382; S.F.C. Milsom, *Historical Foundations of the Common Law*, (London: Butterworth, 1969), p. 372.

[23] *Burrows v. Superior Court*, 13 Cal. 3d 238 (1974).

[24] *Ibid.*; also, *Valley Bank of Nevada v. Superior Court*, 15 Cal. 3d 652 (1975); *Carlson v. Superior Court*, 58 Cal. App. 3d 13 (1976).

procedural requirement would outlaw informal, clandestine, and undocumented access by a government agency to an individual's record, assisting effective oversight of government activity. The second step in curbing voluntary disclosures is to levy a legally enforceable duty of nondisclosure on record keepers who hold records in which an individual has or should have a legitimate expectation of confidentiality. Where records are not the sort the individual has a right to expect will be held in confidence, there is no persuasive argument for making the record keeper liable, though an argument remains for requiring legal process and notice by the government—the tendency to mount fishing expeditions and groundless investigations can only be tempered by effective oversight which requires documentation of investigative activities. But requirements of legal process and notice alone cannot adequately recognize the individual privacy interest in a record.

The second consideration, which emerges from contrasting California law with the traditional status of bank records, is the need to provide the individual with a legally recognized interest he can assert to protect records about himself when government seeks to acquire them from a third party. Granting the individual such an interest gives him (and the record keeper) a basis for limiting voluntary disclosures of such records and forces government to meet certain criteria in order to obtain them. Without such a protectible interest in his records, an individual given notice, standing, and the right to challenge a government request for his records would have little basis for any real challenge, other than to snipe at the facial validity of a summons or subpoena and to question the government's adherence to the proper procedural path. A grant of such procedural defense does not really recognize the privacy interest of the individual; rather, it would create complexity, delay, and expense for all parties while still leading almost inevitably to disclosure to the government. While the requirement that government use formal process and notify the individual when it seeks his records may provide more effective oversight of government activity, procedure alone gives the individual no tool to protect himself. So if one accepts that an individual's bank records are to some extent his private records, creation of a protectible interest, of a legitimate expectation of confidentiality in those records, is essential.

One must not assume, however, that simply passing a statute that provides an individual with a "legitimate expectation of confidentiality" is enough. As the California experience illustrates, further definition of the interest is necessary. Since the expectation in California is constitutionally mandated, the courts there are employing traditional constitutional protections, such as those provided for private papers in the Fourth Amendment, to define the parameters of the expectation. The Commission, on the other hand, in areas where it believes such an expectation needs to be created, has indicated what the definition of that expectation ought to be. For example, in credit, insurance, and medical record keeping, where the vulnerability to government access is similar, the Commission has recommended that an individual be given a legitimate interest in protecting records about him

CamScanner

from unilateral disclosure by the record keeper and, in addition, that he be given a legitimate expectation of confidentiality in such records.

Compulsory Reporting Statutes

The problems of voluntary disclosure of records and access by government through summons or subpoena do not exhaust the varieties of currently legitimate government access to records about individuals that must be considered in fashioning protections for personal privacy. The number of statutes and regulations that require record keepers to collect, maintain, or report information about certain facets of their relationships with individuals mounts steadily and poses grave long-term dangers. In a few situations, the courts have found such compelled reporting and maintenance of records repugnant to Constitutional strictures on government action. Where a statute requires third-party record keepers, such as financial institutions, to supply information from an individual's records to government, or to maintain certain records for government inspection, however, the courts have not extended the Constitutional protections of the Fourth and Fifth Amendments to those records.[25] They are reluctant to do so largely because they still define the reach of individual interest in terms of ownership or possession of a record. This definition also makes courts uncomfortable with extending protection through the self-incrimination standard of the Fifth Amendment, though they have employed that rationale elsewhere to limit government reporting requirements laid directly on the individual.[26]

As long as there is no limit on government requirements that record keepers routinely report information about an individual, circumscribing voluntary disclosures and creating and defining a legitimate expectation of confidentiality would, in the long run, be a hollow protection for personal privacy. An effective protective umbrella must include limits on the manner and extent of government record keeping and reporting requirements.

SCOPE OF THE COMMISSION'S INQUIRY

The Commission's study of government access to records about individuals held by third parties was not limited to the activities of traditional investigative or law enforcement agencies. The Commission examined, in addition, the reporting requirements government has levied on keepers of records about individuals and also the requirements imposed on record keepers to maintain records open to government inspection. Finally, the Commission reviewed the power given a wide variety of agencies not ordinarily equated with law enforcement to compel the production of records for the purpose of assuring compliance with law or maximum efficiency in the delivery of services. This breadth of inquiry reflected the initial understanding of the Commission, confirmed by its findings, that

[25] *Infra*, this Chapter, "Restricting Compulsory Reporting Requirements."
[26] *Infra*, note 125.

information about individuals in the control of one agency tends to become a shared resource, available with little, if any, restriction, to other agencies.

Even with the deliberately wide focus of this study, however, much of the time and resources allocated to the project were spent tracing the practices of investigative agencies. In part, attention to investigative agencies grew out of the traditional concern for abuse in the government's exercise of police powers. The Commission recognized not only that the investigative agencies of government often seem to have an indiscriminate appetite for information about individuals, but also that they tend to be primary exploiters of information held by other agencies for other purposes.

In considering the question of government's exercise of its police powers, one must bear in mind that the ordinary information needs of most agencies of government can be met by seeking information directly from the individual and by inquiries to third parties which the individual authorizes. If a goverment agency satisfies its appetite for information by these means, its appetite can be controlled. Should the government agency act in an improper or unduly intrusive manner, the openness of the process would expose it to remedial action.

Such direct collection occurs where the intent of government is more or less benign; where the concern is supplying a benefit or monitoring compliance with law solely for the purpose of helping people to comply. When government seeks information for the purposes of enforcing compliance with law, however, the agents of government often collect information on their own initiative, through means other than submissions by individuals themselves. Ordinarily, such inquiries are carried out by traditional investigative agencies or by designated investigative or enforcement units of other administrative agencies. These agencies and units can seek the voluntary assistance of third parties who may hold information; or they can employ more powerful tools. The various forms of compulsory legal process, from administrative summons to judicial search warrant, enable agents of government to compel a record keeper to hand over information. On the Federal level, this power is theoretically circumscribed; such inquiries are proper only in response to a statutory command or in the course of investigating violations of statute. In State jurisdictions, investigations of violations of common law also justify the use of compulsory legal process to gather information.[27]

The right of government to mount independent inquiries and employ legal compulsion to secure necessary information is undoubted. The Constitution clearly recognizes the right of government to force the disclosure of information in the Fourth Amendment, but the right recognized is a limited one. The concept of "ordered liberty" which underlies our system of government circumscribes government's right to use its almost unlimited power to compel the production of information.[28] Perplexing and complex problems inherent in this limitation on government

[27] Note, "Common Law Crimes in the United State," 47 *Colum. L. Rev.* 1332 (1947).

[28] See *Entick v. Carrington*, 19 State Tr. 1407 (1765); also, *United States v. United States District Court*, 407 U.S. 297 (1972); *Chimel v. California*, 395 U.S. 752 (1969); *Aguilar v. Texas*, 378 U.S. 108 (1964).

CamScanner

information collection powers emerge most clearly in connection with the operation of investigative agencies.

The independent collection capabilities that government traditionally possesses gave rise to the constitutional and legal standards that are the foundations of our ideas about privacy. Such standards limit the process through which government investigators may exercise their collection powers and, to a more limited extent, prohibit government from collecting and using certain sorts of information. In large part, these restrictions on governmental activity grew out of the notion that the state monopoly on violence inherent in the police power has to be controlled—the individual citizen must not be without protection from the unique coercive powers of the state.[29]

Equally important, the voracious appetite of investigators for information causes them to collect and retain virtually any personal data uncovered unless the collection or retention is *clearly* illegitimate. This attention to avoiding what is improper, rather than accomplishing only what is necessary and proper, leads investigative agencies into abuses of citizens' rights.[30] More often than not, such rights are not clearly protected by the Constitution and have not been secured by statute. As explored earlier, for example, an individual's interest in his bank records is virtually unrecognized, nor does an individual have a right not to have records kept about him except where he is being investigated for violations of law or where he participates in the creation of the record.[31] The basic protections for citizens' rights were fashioned before the emergence of modern investigative agencies with their massive record-keeping systems. The actions of such agencies and their information management practices lend themselves to abuses not apparent when the present protections against government intrusion were developed. Nor was the ability of government to compel the reporting of personal information on a routine basis, and the subsequent capacity of investigators to employ such information for inquiries into an individual's activities, a question to which the nation addressed itself when first considering the protection of personal privacy and autonomy.

In this chapter and in the preceding chapters on record keeping in the private sector, the Commission outlines a policy framework for readjusting the mechanisms necessary to preserve the balance between individual liberty and social order in the light of present conditions. While the focus of

---

[29] See 1 *Annals of Congress* 424-450, 660-779; also, Thomas Jefferson, letter to James Madison, Julian Boyd (ed.), *The Papers of Thomas Jefferson* (Princeton: Princeton University Press,1958), Vol. 12, p. 440.

[30] See, e.g., the activities chronicled in *Intelligence Activities and the Rights of Americans: Book II*, Report of the Senate Select Committee on Intelligence Activities, S. Rep. No. 755, 94th Congress, 2d Session (1976), particularly at pp. 139, 142, 173-74, 178-79, 184, 197-98, 204, 220 (hereinafter cited as "U.S. Senate, Intelligence Activities"); also, the almost inevitable overzealousness of law enforcement investigators has been noted by the Supreme Court frequently, see, e.g., *Johnson v. United States*, 333 U.S. 10, 13-14 (1948); *Aquilar v. Texas*, 378 U.S. 108 (1964).

[31] The Privacy Act of 1974 attempts to set some limits, 5 U.S.C. 552a(e)(1), (e)(2), (e)(7), but, in light of certain exceptions to those limits, the requirements of the Act place few clear limitations on the practices of law enforcement agencies, see 5 U.S.C. 552a(e)(7), (j), (k); also, Chapter 13.

CamScanner

the Commission's attention in this area has been the Federal government, the broad public policy and specific recommendations presented in this chapter are, in the estimation of the Commission, equally applicable to State and local government.

ELEMENTS OF AN EXPECTATION OF CONFIDENTIALITY

Prohibiting Voluntary Disclosure

In several areas of its inquiry, the Commission attempted to identify records about an individual kept by third parties in which it believes the individual should have a legitimate expectation of confidentiality—a right to expect that such records or the information in them would not ordinarily be disclosed without his consent. The Commission found that certain financial, insurance, and medical records fall in this category.[32] The Commission also believes that other areas of private activity, which could not be studied as carefully, create records outside the possession of the individual which deserve protection, one example being telephone toll records.

While toll records are not analogous, as checking account records are, to "private papers" within the meaning of the Fourth Amendment, they provide independent documentation of communications which, before the telephone, were considered uniquely private in character.[33] Indeed, our present legal system severely restricts access to the contents of such communications.[34] Since the mere fact of communication is often as revealing as the content, the Commission believes that toll records should be protected as well. The American Telephone and Telegraph Company has, in fact, already taken a step in that direction by refusing to disclose toll records in all but a few instances unless a subpoena commands it.[35] Moreover, telephone toll records are but one example of areas of record keeping that may be deserving of protection but into which the Commission did not have time to delve.

Whatever the record about an individual, however, if it is determined to be one in which a legitimate expectation of confidentiality should exist, then to secure that expectation the record keeper must be put under a duty not to disclose the information in the record without the consent of the individual unless required to do so by legal process or government reporting requirements. Simply saying that a record keeper may not disclose voluntarily, however, is not enough. Real protection demands that the individual have the means to prevent improper disclosures by a record keeper and secure redress against a record keeper who violates the basic

[32] See Chapters 2, 3, 5, and 7.

[33] See Alan F. Westin, *Privacy and Freedom*, (N.Y.: Atheneum, 1967) p. 330; *Commonwealth v. Lovett*, 4 Clark 5 (Pa., 1831).

[34] *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967); 18 U.S.C. 2510 *et seq.*

[35] Except in so-called "national security" situations; see Testimony of American Telephone and Telegraph Company, Credit-Card Issuers Hearings, February 12, 1976, pp. 46-50; letter from H.W. William Caming, Attorney, AT&T, to the Privacy Protection Study Commission, August 13, 1976, p. 2.

CamScanner

expectation of confidentiality. To an extent, the mode for obtaining such redress is set out in the Commission's recommendations regarding particular areas of record keeping. A critical further step is clear definition of the individual's legal interest in the record, of his expectation of confidentiality as it applies to the question of voluntary disclosure by the record keeper.

Under existing law, when documentary information is voluntarily supplied to law enforcement personnel in the course of investigation, such as wage records provided by an employer, the subject of such documentary evidence is presumed not to have a legal interest in the records. As the Supreme Court has noted, personnel files and the like are "records in which the . . . [individual] has no proprietary interest of any kind, which are owned by the third person, which are in his [third person's] hands, and which relate to the third person's transaction" with the individual.[36] For these reasons, the record keeper's right to volunteer the information in its records to the government is currently unrestricted.[37] Even documents obtained illegally by private parties, if acquired without government knowledge or complicity, may be turned over to and used by the government.[38]

As explored earlier in this chapter, and in several other sections of this report, not only is the record keeper free to disclose as a matter of theory, record keepers in sectors such as banking and credit make a practice of disclosing account information voluntarily to government agents. The Commission's survey of credit-card issuers and their disclosure practices confirmed testimony to this effect received during the Commission's hearings.[39] Representatives of Federal investigative agencies themselves corroborated the Commission findings that, with the exception of requests for telephone toll records and the records maintained by a limited number of banks, most of the requests they make for records are complied with informally. Frequently, government agencies maintain informal liaison with credit companies and banks to facilitate the flow of account information.[40]

These findings reinforce the conclusion that only when an individual can claim a legal interest equal to the California standard of a legitimate expectation of privacy is voluntary disclosure of his records by third-party record keepers securely limited. Recognition of such a legal interest places clear responsibility on the record keeper to assure against improper disclosure, to government or anyone else. If information is improperly disclosed, in other words, the record keeper is liable for damages or susceptible to injunctive relief. The fact that the record keeper is liable for improper disclosures of information held confidentially, however, does not mean that the government may use informal coercion to force "voluntary" disclosure, thus escaping liability. Indeed, if government were to coerce

---

[36] *Donaldson v. United States*, 400 U.S. 517 (1971).

[37] *Infra*, this Chapter, "Regulating the Compelled Production of Records."

[38] *Burdeau v. McDowell*, 256 U.S. 465 (1921).

[39] *Supra*, notes 15-19; Chapter 2, "The Consumer Credit-Relationship"; also, the ease with which government agents gain access to private records held by third parties was confirmed in interviews with officials of Federal investigative agencies conducted by Commission staff.

[40] Staff interviews with Special Agents of the Federal Bureau of Investigation, at Headquarters, Washington, D.C. on January 6,1977.

CamScanner

disclosure, there would be little equity in holding the record keeper responsible. The Commission believes that as a corollary to prohibitions on voluntary disclosure by record keepers, stringent penalties should be established for inducing a record keeper or its employees to disclose information in which an individual has an expectation of confidentiality. Such an enforcement scheme should include the right to initiate an individual civil damage action against anyone who induces the breach of an expectation of confidentiality in records. The scheme should extend sanctions to all persons, not simply government agents.

A record keeper's duty not to disclose recorded information in which an individual has a legitimate expectation of confidentiality should not prohibit every disclosure. Obviously, there are circumstances in which the record keeper should have the discretion, or even the duty, to disclose. If the record subject injures the record keeper, for example, information may be disclosed by the record keeper to establish the fact of injury or to assist those investigating the injury. Protecting privacy does not mean completely insulating an individual; if he violates the terms of his relationship with a credit-card issuer, for example, he must be prepared to accept the costs of injury to that financial agent. In such circumstances, the record keeper should be free to disclose information about the individual necessary to assure full compensation for the injury and proper application of the law.

In addition, if a record keeper becomes aware from information generated in its relationship with an individual that he is engaged in illegal activity, then the record keeper should be under some obligation to disclose that information to proper authorities, as would any other citizen. For example, if a bank holds confidential documentary information which indicates that an individual is engaged in illegal transfers of funds to a foreign nation, the bank might be implicated as an accessory if one of its officers were aware of the transfer and the bank did not report it.[41] It is not the intent of the Commission to create a new testimonial privilege for bankers, insurers, or anyone else. Rather, the Commission seeks to fashion protection for *documentary* information about individuals which, were it not for Twentieth Century changes in social and economic organization, would have remained the private and protectible records of the individual. The observations of the record keeper and his employees concerning the actions of the individual which appear to be illegal are not, in the Commission's opinion, protectible information.

Finally, as outlined in the credit, depository, insurance, and medical records recommendations of the Commission, certain disclosures by the record keeper are necessary to maintain properly the relationship between record keeper and individual. Within the context of the prior notice provisions and redisclosure safeguards recommended in the chapters

[41] e.g., 18 U.S.C. 4; also, *Tournier v. National Provincial Union Bank* (1924), 1 K.B. 461, 473, 481 (C.A.).

CamScanner

dealing with those types of records, the Commission recognizes the legitimacy of such disclosures.[42]

A prohibition on voluntary disclosure provides the first element in the design of the expectation of confidentiality which the Commission recommends for certain records. To secure this first portion of the legal barrier that will protect records about an individual from improper incursion by government and others, the Commission recommends that as a general rule a private-sector record keeper maintaining records in which an individual has a legitimate expectation of confidentiality should not disclose information from such records without the consent of the individual, except under the specific circumstances discussed in the last few pages and articulated in the separate recommendations relating to each area of private-sector record keeping.

Concurrent with this limitation, the Commission, of course, recommends restrictions on how government may go about obtaining information about individuals from third-party record keepers. Those limitations on government access will be discussed below.

Regulating the Compelled Production of Records

> We thus conclude that under the statutes here applicable . . . that today that which we have previously considered to be administrative fishing expeditions are often permitted; and that administrative subpoenas may be enforced for investigative purposes unless they are plainly incompetent or irrelevant to any lawful purpose.[43]

The quotation above from a recent opinion of the United States Court of Appeals for the Tenth Circuit symbolizes the relative ease with which the Federal government today may compel the production of records about individuals. Whatever the scope or purpose of a subpoena, be it an administrative or judicial summons, compulsory process to obtain documentary information about an individual from a third party who maintains a record about, or on behalf of, that individual is virtually unchallengeable. Equally important from the perspective of safeguarding individual rights, certain portions of the process by which some judicial or administrative summons may be issued need reconsideration.

Though the Commission is most directly concerned with problems engendered by government access to records about individuals held by third parties, this examination of summons and subpoena power pays more than passing attention to the procedure by which any compulsory process is issued, whether to the individual or to an independent record holder. In large part, this scope of inquiry is appropriate because distinguishing between types of legal process on the basis of who receives the process would be spurious in procedural terms.

The processes of compulsion at the Federal level which the Commis-

---

[42] See Chapter 2, *Recommendation (12)*; Chapter 3, *Recommendation (8)*, Chapter 5, *Recommendation (17)*, Chapter 7, *Recommendation (10)*.

[43] *EEOC v. University of New Mexico*, 504 F.2d 1296, 1301 (10th Cir. 1974).

sion scrutinized fall into three broad categories: (1) administrative summons, (2) judicial subpoenas in the course of litigation, and (3) Grand Jury subpoenas. These and the search warrant are the forms of legal process the Federal government uses to compel the production of records or testimony. The Commission is well aware of the bewildering variety of administrative tools, from "inspection warrants" to "subpoenas," which fall under the umbrella term, "summons." But as the discussion below explains, the Commission found good reason to treat all such processes similarly.

Before examining the forms of administrative summons and judicial subpoena, however, two questions must be disposed of: the definition of an individual's legal interest in records which he has a right to consider confidential; and, the rationale of the Commission in not including the use of the search warrant in its considerations.

Definition of an Individual's Legal Interest

As the earlier portions of this chapter illustrate, an individual currently has no legally recognized interest in certain records about him, though these records may be ones in which the Commission has found that he ought to have an expectation of confidentiality.[44] Without that legal interest, or "legitimate expectation of privacy" as the courts have termed it, the individual has no basis to challenge access to those records by government; that is, no ability to protect his expectation of confidentiality. Whether access to information about an individual is demanded by Grand Jury subpoena to a bank,[45] by administrative summons to an accountant or employer,[46] or by a subpoena during litigation directed to third parties, the individual is without standing to contest and, even if he were given standing, without substantive protections, constitutional or statutory, which he might assert.

Attempts to provide the individual with protection through mere procedural reform are, unfortunately, ineffective. The Tax Reform Act of 1976,[47] for example, provides a mechanism that was meant to help individuals protect records in third-party hands from the administrative summons of the IRS. The mechanism, however, does not accomplish that purpose (though it does provide means for oversight of agency activity by other institutions). The Tax Reform Act requires the IRS to give an individual notice that a summons has been served on a third-party record keeper and allows the individual both to stop the record keeper from complying until a hearing is held and to intervene in any hearing or enforcement proceeding. Such a notice, with standing and nothing more, while it may deter baseless investigative activity, gives the individual little with which to impede IRS access. In short, the recent amendments to the tax code do not alter the inability of an individual to protect records about him held by third parties, even in the limited context of IRS summonses. To be

[44] *Supra*, notes 10, 42.
[45] *United States v. Miller*, 425 U.S. 435 (1976).
[46] *Couch v. United States*, 409 U.S. 322 (1973); *Donaldson v. United States*, 400 U.S. 517 (1971).
[47] 26 U.S.C. 7609.

sure, the individual may go into court, but when he gets there he has nothing to say, because he has no legal interest to defend or to balance against the government's desire for the record.

The rationale for leaving the individual helpless in this situation was best articulated in the *Miller* decision; because he does not possess and control the records, the individual has no "proprietary" interest in them and, thus, no protectible legal interest of any sort, at least against the government.[48]

The emphasis the Supreme Court laid on the possessory relationship of the individual to the record in *Miller*, however, need not frustrate efforts to fashion a legally protectible interest for the individual. Previous Supreme Court decisions, in fact, had suggested that such an interest might be found. In *Donaldson v. United States*,[49] the Court rejected an employee's attempt to challenge an IRS summons for certain employment records because the summons was not directed to records "in the hands of anyone with whom the taxpayer had a confidential relationship of any kind"; the records sought were ones "in which the taxpayer has no proprietary interest of any kind, which are owned by the third person, which are in his [the third person's] hands, and which relate to the third person's business transactions with the taxpayer."[50] In short, the records sought were not held by someone from whom the individual might claim any duty to hold the record in confidence.[51] The Court did not, in *Donaldson*, restrict the possible reach of the individual's interest to possession alone. In a line of cases which the Court distinguishes from those involving records,[52] it recognized an interest in information not possessed or controlled by the individual.

Rejecting the notion that geographic suzerainty or a "proprietary" interest is necessary to protect communications from interception without a search warrant, the Supreme Court indicated in *Katz v. United States* that even without such traditional interests an individual had a legitimate expectation of privacy.[53] The Court noted that "the premise that property interests control the right of the government to search and seize has been discredited."[54] Thus, a legal and logical basis exists for recognizing an individual interest in records about him held by third parties, but the parameters of that interest have yet to be defined.

In the definition emerging as the California courts apply that State's constitutional protection for a "legitimate expectation of privacy" in bank records, the Commission sees the outline of the protectible legal interest that

---

[48] Against a private party, he may have some interest, in contract or through certain "common law" expectations; see *Milovich v. First Nat'l Bank*, 224 So.2d 759 (Fla. Ct. App. 1969); *Sparks v. Union Trust Co.*, 256 N.C. 478 (1962); *Peterson v. Idaho First National Bank*, 83 Idaho 578 (1961); also, *Brex v. Smith*, 104 N.J. Eq. 386 (1929).

[49] 400 U.S. 517 (1971).

[50] *Ibid.*, at 523.

[51] *Supra*, note 5.

[52] *Warden v. Hayden*, 387 U.S. 294, 304 (1967); *Berger v. New York*, 388 U.S. 41 (1967); *Katz v. United States*, 389 U.S. 347 (1967); for the distinction of "records" from "communications," see *Couch v. United States*, 409 U.S. 322 (1973); *United States v. Miller*, 425 U.S. 435 (1976); *Fischer v. United States*, 425 U.S. 391 (1976).

[53] 389 U.S. 347 (1967).

[54] Citing *Warden v. Hayden*, 387 U.S. 294 (1967).

CamScanner

will safeguard the individual while permitting the effective enforcement of law necessary for an ordered society. While the legal expectation enjoyed by an individual in California was first recognized in 1974 in *Burrows v. Superior Court*,[55] the substance of that expectation did not begin to emerge clearly until a year later in *Carlson v. Superior Court*.[56] Giving content to the expectation recognized by the California Supreme Court in *Burrows*, the California Court of Appeals (4th District) ruled that, "law enforcement officials may not gain access to an accused's private papers [in this case, bank records] by subpoena until there has been a judicial determination that there is probable cause to believe he has committed a criminal offense and that the papers and documents described in the subpoena would be material evidence in the case."[57] In other words, the Court of Appeals suggested that the State must establish both probable cause to believe a crime has been committed and the relevance of the records sought to that crime before the privacy interest of the individual in the records can be overborne.

The Commission endorses this approach, believing that records in which an individual has an expectation of confidentiality should not be accessible to government unless a compelling governmental interest, outweighing the individual's interest to be free from government intrusion, can be shown.

RECOMMENDATIONS

The first step in securing such an expectation was examined earlier in this chapter—the record keeper maintaining a confidential record must be placed under a duty not to disclose the record without the consent of the individual, except in certain limited circumstances. The specific limitations placed on record keepers in such areas as financial services,[58] medical care and insurance are set out elsewhere in this report.[59] Coupled with these obligations on third-party record keepers must be certain limitations on government action and certain rights which the individual can assert. Thus, as the second step in securing the expectation of confidentiality, the Commission recommends:

Recommendation (1):

That Congress provide an individual by statute with an expectation of confidentiality in a record identifiable to him maintained by a private-sector record keeper in its provision of financial services, medical-care, insurance, or telecommunications services, which statute should specifically require that the individual, in defense against compelled

[55] 13 Cal.3d 238 (1974).
[56] 129 Cal. Rptr. 650 (1976).
[57] *Ibid.*, at 655.
[58] The terms "financial service" and "financial institution" should be understood to mean those services and institutions covered by the recommendations of the Commission in Chapter 2, "Consumer-Credit Relationship," and Chapter 3, "The Depository Relationship."
[59] See Chapter 2, *Recommendation (12)*; Chapter 3, *Recommendation (8)*; Chapter 5, *Recommendation (17)*; Chapter 7, *Recommendation (10)*.

CamScanner

production of such a record pursuant to any administrative, judicial, or legislative summons, subpoena, or similar order be permitted—

(a) to challenge the relevance and scope of the summons, subpoena, or order and to require from the government clear proof of the reasonable relationship of the record sought to the investigation, prosecution, or civil action in furtherance of which the summons, subpoena, or order was issued before a court may order disclosure of the record; and

(b) to assert in protection of the record the protections for private papers and effects articulated in the Fourth Amendment, and the due process protections articulated in the Fifth Amendment, to the Constitution of the United States.

The Commission recognizes that the recommended measure does not reach fully the level of protection afforded an individual under California law. Section (b) of the recommendation creates a standard that may amount to somewhat less than probable cause; what the Commission recommends may not raise all requests for bank, credit, insurance, or health records to the level of a search warrant.[60] At the very least, however, it will force government to establish reasonable cause to believe that the record is relevant to prosecution of a violation of law before the legitimate expectation of the individual can be overridden.[61]

Search Warrants

Turning from the definition of the legal substance of an individual's expectation of confidentiality, the question of search warrants can now be reviewed briefly. The protections against abuse of the search warrant by government officials are articulated in the Fourth Amendment to the Constitution.[62] For a magistrate to issue a warrant, the government must establish probable cause and describe with specificity the place to be searched and the materials to be seized. Although, in the search warrant situation, the individual has no opportunity to contest seizure of the records beforehand, he may be able to suppress the use of the information afterward, since government must meet the requirements of the Fourth

[60] See *Andresen v. Maryland*, 427 U.S. 463 (1976); *Beckwith v. United States*, 425 U.S. 321 (1976); *Fisher v. United States*, 425 U.S. 391 (1976); *United States v. Bisceglia*, 420 U.S. 141 (1975); given that an individual will have the right to challenge the summons before it can be enforced, a relativistic balancing test of government need and individual right will surely emerge, rather than a strict standard such as probable cause being placed on government.

[61] If the standards of *Bisceglia* and *EEOC v. University of New Mexico* are to be tightened at all, this is the minimum test government would have to meet.

[62] *The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons and things to be seized. U.S. Const.*, amend. IV.

Amendment in order to employ the fruits of the warrant as well as to procure it.[63] Should the government act in violation of the constitutional strictures, clear channels for redress exist.[64] To the extent that requiring government to present a compelling need for a particular record helps secure an individual's expectation of confidentiality, the search warrant provides adequate protections.

Given probable cause, however, the government may employ a search warrant today to seize virtually any record about an individual, whether held by the individual or by a third party. No longer do there seem to be any personal documents inaccessible to government because they reveal "intimate areas of personal affairs."[65] The notion has vanished that some documents are as deserving of absolute protections as are the utterances protected absolutely through the combined strictures of the Fourth and Fifth Amendments.[66] Today, whatever a person may write down, to prepare his taxes or settle his mind, meant for only a few others or for no one else's eyes, government can have if government acts through the proper procedures. While this element of contemporary constitutional interpretation does not unduly disturb the Commission in regard to the records about individuals ordinarily kept by third parties in the course of a confidential relationship with an individual, such as bank records, the idea that papers in the hands of the individual have no sanctity is troubling. The Commission focused on more or less formalized record keeping in its study; it is unsure of how to go about defining the sort of papers that should be inviolate in the hands of the individual but urges the Congress, the courts, and legal scholars to continue working to resolve this issue and to mark out a clearer zone of impenetrable personal privacy.

Having proposed that the individual's interest in certain records be legally recognized, and having suggested that certain records which are personally held may need absolute protections, the Commission turned its attention to the procedures, legal and practical, by which government exercises its power to compel access to records.

Prohibition on Informal Access

Returning for a moment to the question of informal access to personal records by government, the Commission's study showed that a wide variety of records about individuals are revealed to government without leaving a

---

[63] See *Mapp v. Ohio*, 367 U.S. 643 (1961); *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971); Oaks, "Studying the Exclusionary Rule in Search and Seizure," 37 *U. Chi. L. Rev.* 665 (1970); also *Katz v. United States*, 389 U.S. 347 (1967); *United States v. United States District Court*, 407 U.S. 297 (1972); see further (re: force and fraud), *Ker v. California*, 374 U.S. 23 (1963).

[64] *Mapp v. Ohio*, 367 U.S. 643 (1961); *Bivens v. Six Unknown Named Agents*, 403 U.S. 388 (1971).

[65] See *Andresen v. Maryland*, 427 U.S. 463 (1976); *Fischer v. United States*, 425 U.S. 391 (1976); *Boyd v. United States*, 116 U.S. 616 (1886); Note, "Formalism, Legal Realism . . .," 90 *Harv. L. Rev.* 945.

[66] See *Boyd v. United States*, 116 U.S. 616 (1886); and Note, "Formalism, Legal Realism. . ." 90 *Harv. L. Rev.* 945.

CamScanner

record that the disclosure was made and without the individual ever being aware of the disclosure.[67] While documentation of such disclosures will not directly help the individual protect his records, it will help in discovering improper or excessive acquisition of information by government. Access by Federal investigators to the records of private associations, retailers, employers, or local government agencies, for example, where government need not use compulsory process because there is no expectation of confidentiality, could be monitored. Such public documentation and consequent ability to monitor investigative collection activities may help to avert the dangers of clandestine compilation of unnecessary records such as those discovered in 1976 by the Senate Select Committee on Intelligence Activities.[68] To effect such documentation of government requests for personal records, the Commission, therefore, recommends:

Recommendation (2):

That any request for an individually identifiable record made to a private-sector record keeper or agency of another government jurisdiction by a government agency or its agents be made only through recognized legal process, such as an administrative summons or judicial subpoena, unless the request is made with the consent of the individual to whom the record pertains.

The Commission does not intend through this recommendation to cut off an investigator's ability to seek the testimony of parties with whom an individual under investigation may have had contact; nor does it want to eliminate the ability of the retailer, for example, to refresh his memory of contact with an individual from his own records. When government seeks a *copy* of a record, such as the charge record from a gas station or the hotel's copy of a guest's bill, it would have to use legal process. The Commission sees no reason why government should not leave a paper trail of its investigation just as the individual in our society leaves a trail of his activities. The value of personal records to agencies investigating the legitimacy of an individual's conduct suggests that similar documentation of government information collection activities will be equally valuable for investigating and assessing the legitimacy of governmental conduct. Finally, it should be recognized that requiring government to use legal process to obtain individually identifiable records does not mean that the individual can halt such access or create delays where he has no legitimate expectation of confidentiality in the record.

What are those forms of process which government must employ to obtain records, however; and, what limits does the Commission recommend placing on them? As outlined at the beginning of this section, government moves to obtain documentary evidence through three basic forms of process: administrative summons, judicial subpoena in the course of

[67] *Supra*, notes 15-19, 35, 40.
[68] U.S. Senate, *Intelligence Activities*, generally pp. 137-288.

litigation, and Grand Jury subpoena. There are common elements in the way the three are issued.

The Subpoena and Summons

A subpoena or summons is simply a form which a government agent or attorney fills in to show who is commanded to appear, with what document or testimony, when, and where. For an administrative summons, the form is prepared by the agency for which the official filling it out works. For a judicial or Grand Jury subpoena, the form is obtained simply by asking the clerk of a district court for a blank. U.S. Attorney's offices, for example, often have boxes of blank Grand Jury subpoenas on hand. After it is filled in, the subpoena or summons is delivered to the person to whom it is directed, or the "addressee," who may comply with it, and, if he wishes, hand over the records requested immediately or as soon as he can get them together. The addressee, however, may decide not to comply with the request. If he refuses, the government must then take the matter before a magistrate if it wants to compel the addressee to disclose the specified information. At that point the addressee can challenge the propriety of the subpoena, either on the grounds of procedural deformity or on the basis of some protected legal interest he has in the information. The magistrate then determines the validity of the subpoena or summons and, if valid, orders the addressee to produce the information or be punished by fine or imprisonment. As this synopsis illustrates, the executive agency or investigator issues and delivers a summons or subpoena without prior judicial supervision or even knowledge; supervision comes into play only if the subpoena is challenged and there is a legally recognized basis for that challenge.[69]

If personal records are in the possession of the individual, as they usually were when the subpoena process developed,[70] a subpoena does not threaten the confidentiality of those records unduly. The individual could go into court and seek to stop unwarranted government seizure of his records. With so many personal records not within the individual's possession, and with the courts generally refusing to recognize the interest of the individual in records he does not possess, the subpoena and summons allow government to seize personal records without the possible intervention or even knowledge of the individual. Nor does the process allow the record keeper to assert a privacy interest for the individual or to raise questions which go much beyond whether the subpoena was filled out properly.[71] In effect, the subpoena has become a tool that government agents can use to seize the records of an individual without being required either to give him an opportunity to dispute this action before his privacy is invaded or to

[69] See, e.g., *United States v. Miller*, 425 U.S. 435 (1976); *Donaldson v. United States*, 400 U.S. 517 (1971); *United States v. Powell*, 379 U.S. 48 (1964).

[70] Theodore F.T. Plucknett, *A Concise History of the Common Law*, (5th Ed., Boston: 1956), pp. 683-684.

[71] *California Bankers Assn. v. Schultz*, 416 U.S. 21, 53 (1974); *United States v. First Nat'l Bank of Mobile*, 295 F.142, 143 (S.D.Ala. 1924), *aff'd, per curiam*, 267 U.S. 576 (1925).

CamScanner

establish a reasonable basis for the seizure (i.e., probable cause) before an impartial magistrate.[72] The protections of the Fourth Amendment against unreasonable search and seizure, meant to give individuals the assurance that the executive could not act in a high-handed and unchecked manner, seem to have been superseded. The procedures by which the various forms of subpoena and summons are issued tend to exacerbate this problem of unreviewed executive action. Government investigators today may decide what information they need and seize it without prior outside supervision.

The Administrative Summons

The Commission reviewed more than 160 separate statutes which empower Federal authorities to compel the production of documents or records.[73] Though this sample represented a large proportion of the statutes granting some sort of summons power at the Federal level, it was by no means exhaustive.

The procedures by which administrative summons power is exercised ordinarily parallel those for issuing, serving, and adjudicating challenges to a judicial subpoena, whether the summons power is provided by statute to conduct investigations or to assist in adjudication of claims before an administrative tribunal. The term "administrative summons" as employed in this report, however, also encompasses broad record inspection powers under which an agency need employ no document to gain access to a record, at least so far as the statutory grant of power is concerned.[74]

Whatever the nature of the summons power in a particular case, however, the Commission found that it is uniformly given to administrative bodies who have enforcement or oversight responsibilities—in other words, to virtually every agency of government. The reach of such summons power is restricted to the compulsion of information which is arguably relevant to carrying out an agency's responsibilities.[75] The restriction, however, need not mean much. An IRS summons issued in a tax investigation, for example, may reach to any conceivable record about an individual. As U.S. Supreme Court Justice Stewart noted in reviewing IRS summons power in 1975,

> virtually all persons or objects in this country may, of course, have Federal tax problems. Everyday the economy generates thousands of sales, loans, gifts, purchases, leases, deposits, mergers, wills, and

[72] See particularly the discussion of the use of the Grand Jury Subpoena *infra*.

[73] Most of the statutes reviewed were the product of a computer search conducted for the Privacy Protection Study Commission by the Congressional Research Service of the Library of Congress. A few of the statutes examined were obtained through manual research by Commission staff. Throughout this section of the text on Administrative Summons, the statutes cited in notes ordinarily will be examples of statutory structure and language rather than an exhaustive list of all Federal statutes which might illustrate the point at issue.

[74] 15 U.S.C. 49; 21 U.S.C. 880.

[75] The tenuous nature of the relevance which is necessary is illustrated in *United States v. Powell*, 379 U.S. 48 (1964); also, *FTC v. Texaco, Inc.*, 517 F.2d 137, 170 (D. C. Cir., 1975).

CamScanner

> the like which suggest the possibility of tax problems for somebody. Our economy is tax relevant in almost every detail.[76]

The sources which may authorize the issuance of the summons run the gamut from the majority of the members of a governmental agency to any person designated by the highest official of the agency. Statutes grant the right to issue a summons to the following: agency, committee, subcommittee; chairman, president; vice-chairman, nondesignated committee member, designated committee member; designated department head, designated officer, designated representative, designated employee; examiner, claims agent, collections agent, appraiser, proper United States attorney, attorney representing the government, any agent of the FBI, any designated employee of any State, territory, or political subdivision; or, any designated person.[77]

Few of the statutes specify who must sign a summons in order for it to issue. The laws which do specify most often delegate the power to the chairman (or other head official) or individuals he may designate. Some statutes also go so far as to mention who may deliver the summons, but most of those simply permit delivery by any individual whom the issuer designates.[78] There is no statutory attempt to keep the power to issue a summons in the hands of those with supervisory responsibilities.

The range of records which may be compelled by an administrative summons is also broad. Many statutes simply grant the power of subpoena or of subpoena *duces tecum* without elaboration.[79] Others add such brief, general descriptions as "information," "records," or "documentary evidence." Others enumerate lengthy lists of compellable evidence, e.g., "books, papers, schedule of charges, contracts, agreements, or documents." The most common combination of words used in statutes is the phrase "books, papers and documents."[80]

A few statutes, but only a few, establish express limitations on summons power by excluding certain records from the reach of the summons. For example, the enabling legislation of the Food and Drug Administration gives broad powers to inspect records which are required to be kept by law and related documents, but specifically excludes financial data, sales data other than shipment data, or pricing data.[81] Ordinarily when statutes specify direct limitations on the summons power, they only reiterate common law or constitutional principles which would be applicable anyway, reaffirming preexisting limitations. In contrast, a few statutes establish additional procedural rights and set forth requirements of nondisclosure.[82]

The rare statute that prohibits disclosure does so to protect confiden-

---

[76] *United States v. Bisceglia*, 420 U.S. 141, 154 (1975) (Stewart, J., dissenting).

[77] 22 U.S.C. 1623; 12 U.S.C. 1464(d)(9); 7 U.S.C. 15, 115, and 136d; 15 U.S.C. 1173; 42 U.S.C. 405.

[78] 15 U.S.C. 4a.

[79] 12 U.S.C. 1464(d)(9).

[80] Over 20 percent of the statutes reviewed employed that phrase.

[81] 21 U.S.C. 880.

[82] 7 U.S.C. 87f; 18 U.S.C. 1968; 21 U.S.C. 374; 29 U.S.C. 161.

CamScanner

tial subject matter or trade secrets. In addition, the Freedom of Information Act articulates several reasons which justify a refusal to disclose specifically requested information. These statutes limit the conditions under which disclosure may be made. At least one permits disclosure to anyone if dissemination will aid the individual who gave the information.[83] Under most of the statutes granting summons power, however, the executive agency has virtually unlimited discretion to determine what information is sufficiently confidential or private to trigger nondisclosure requirements.[84]

In a majority of cases where statutory language limits the summons power, a broad "reasonableness" standard is employed. The statutes mandate that a summons be reasonable with respect to particularity, timeliness, and relevance (e.g., location, identity of custodian, good faith belief that the individual possesses the records). Fair housing legislation provides one example:

> The Secretary (of HUD) shall grant the petition (of the witness) if he finds that the subpoena requires appearance or attendance at an unreasonable time or place, that it requires production of evidence which does not relate to any matter under investigation, that it does not describe with sufficient particularity the evidence to be produced, that compliance would be onerous, or for other good reason.[85]

Some five percent of the statues reviewed contained this kind of limitation.

Rather than limiting administrative summons power, many statutes expand its reach even beyond the range permitted through judicial subpoena power. They increase government's ability to obtain information by restricting the scope of privileges, broadening inspection powers, increasing protection of informants, and offering preferential treatment for the agency seeking the information.[86] As discussed later in connection with government information reporting and record-keeping requirements, the statutory expansion of administrative ability to compel disclosure of information includes the power to enter and inspect records without even the formality of an official piece of paper.[87]

In effect, the scope and use of administrative summons power is left largely to administrative discretion. While most administrative summons do not appear to have been misused, only the goodwill and restraint of the innumerable officials empowered to issue and administer summons protect an individual from abuse. Unfortunately, some abuses of power have occurred.

The agents of the Internal Revenue Service, for example, have

---

[83] 45 U.S.C. 362.

[84] A few statutes do modify this ability by permitting the individual who is compelled to provide information to initiate an agency determination regarding what information may not be disclosed, though ordinarily only in the context of trade secret and similar information. See, e.g., 50 U.S.C. App. 6430.

[85] 42 U.S.C. 3611.

[86] 12 U.S.C. 1784; 15 U.S.C. 155.

[87] *Supra*, note 74.

exercised their power to issue summons in questionable and improper ways.[88] Former Commissioner Alexander attempted to prevent further abuses by restructuring the internal procedures for the issuance of a summons. At the same time, similar misuse of process by other agencies has not led to internal reform.[89] Even were administrative reform comprehensive, however, the individual cannot be sure of protection unless the Congress acts. Dependence on the restraint of executive officers alone is perilous.[90]

In addition to the dangers cited, the possibility of information flowing indiscriminately from the agency acquiring it to others leads to abuses of the administrative summons power. It is not only the information produced through reporting requirements which circulates widely within government; information obtained by agencies through their summons power for a specific purpose also flows to other agencies for unrelated use. As former Deputy Attorney General Tyler indicated to the Commission, information in the hands of the IRS, whether compelled through a reporting requirement or the summons power, is viewed as a general governmental resource.[91]

The courts have not acted to restrain the scope of administrative summons power, although some judges have expressed discomfort with the notion that "unreviewed executive discretion" may result in disclosure of records of "intimate areas of personal affairs" which could violate an individual's legitimate expectation of privacy.[92] However uncomfortable they may be, though, judges, especially the Supreme Court, have endorsed the expanding reach of administrative summons power.[93] Virtually no individually identifiable record in the control of a third-party record keeper is immune from an administrative summons; and, the individual is without a legally recognized interest which he may assert to protect a record about himself, even if it is a bank, credit, employment, insurance, or medical record. Furthermore, the present ability of government to compel disclosure of records administratively is so broad and ill-defined in scope that it permits what the Tenth Circuit characterized as "fishing expeditions" and what Justice Stewart has suggested is compulsory process based on "sheer speculation."[94]

In order to minimize the dangers created by the current unrestricted and ill-defined administrative summons power of Federal agencies, and to return to the individual some measure of control over records about him held by third parties, the Commission recommends:

---

[88] *Supra*, notes 15, 16, 18.

[89] Testimony of the Internal Revenue Service, Depository and Lending Institutions Hearings, April 22, 1976, pp. 785-86; *The New York Times*, April 20, 1975, IV, p. 4:5; June 11, 1975, p. 29:6; June 21, 1975, p. 1:5; also, S. Rep. No. 938, 94th Cong., 2d Sess., pp. 368-369 (1976).

[90] U.S. Senate, *Intelligence Activities*, pp. 14-15.

[91] Testimony of the Deputy Attorney General, United States Department of Justice, *Federal Tax Return Confidentiality*, Hearings before the Privacy Protection Study Commission, March 11, 1976, pp. 63-65.

[92] *California Bankers Assn. v. Schultz*, 416 U.S. 21, 78 (1975) (Powell, J., concurring).

[93] See, e.g., *United States v. Bisceglia*, 420 U.S. 141 (1975).

[94] *Ibid.*, at 158 (Stewart, J., dissenting); *EEOC v. University of New Mexico*, 504 F.2d 1296, 1301 (10th Cir. 1974).

CamScanner

Recommendation (3):

That Congress provide by statute that an administrative summons (or other form of compulsory legal process) issued by an administrative or executive authority of government to a private-sector record keeper in order to inspect or obtain an individually identifiable record shall be issued only

(a) for the inspection of a record required to be maintained pursuant to a statute or regulation, or

(b) for the investigation of violations of law where the evidence obtained by such administrative summons (or other form of compulsory process) will be used only for administrative action, civil enforcement, or criminal prosecution directly related to the statutory purposes for which such summons power was granted, except, where evidence of unrelated criminal activity is uncovered, the existence of such activity may be reported to a proper investigating authority who may then proceed to obtain such information from the record keeper pursuant to whatever legal processes are at its command; and

(c) where a copy of the administrative summons is served by the administrative or executive authority of government upon an individual who (i) is, or is likely to become, the subject of investigation or enforcement proceedings, and (ii) is the subject of the record to be produced,

(d) where the issuance of such a summons may only be made by officials of the issuing agency who are not field agents and who exercise supervisory authority and responsibility over the agents who will serve the summons, and

(e) where an individual identified in the record and subject to notification under (c) above has standing to assert protections for those records in which he has an expectation of confidentiality as defined in *Recommendation (1)* above or any other defense provided by common law or statute;

except that,

(f) an administrative summons may be issued without service upon the individual where the government shows to a court that service would:

- **(i) pose a reasonable possibility that the record sought will be destroyed, or an attempt to destroy it will be made, by the record subject upon whom service of the summons is required; or**
- **(ii) pose a reasonable possibility that other evidence would be destroyed or become unavailable to government, jeopardizing the investigation; or**
- **(iii) cause flight from prosecution by the individual upon whom service of the summons is required; or**
- **(iv) endanger the life or physical safety of any person;**

CamScanner

provided that, before issuance of such a summons, the government must show the reasonable relationship of the record sought to the investigation in furtherance of which the summons is to be issued. Within a reasonable period of time after issuance of a summons without notice, the government must notify the subject of the record of the seizure. This provision ((f)) would not, however, apply to a record in which an individual has a legitimate expectation of confidentiality recognized by statute or common law.

The Commission believes that this recommendation would curtail the potential for invasion of personal privacy through unreviewed executive action. It would limit the unmonitored expansion of administrative summons power and return the decision to compel disclosure of documents to the supervisory level, where it belongs. In addition, the recommended measure would interfere little with the proper activities of law enforcement. While some inefficiency inevitably occurs when one seeks to safeguard personal privacy, the provisions of subparagraph (f) will minimize any additional burden on government. Finally, the Commission appreciates the arguments of law enforcement officials who suggest that motions to quash summons will result in delays, largely because of protracted appeals.[95] To avoid a potential bottleneck, the Commission suggests that a district court decision regarding enforcement of a summons should not be a final judgment from which an individual could take an interlocutory appeal, but should be appealable only as an evidentiary question after prosecution. Or, if no prosecution is brought, then an individual would be entitled to appeal the decision on the summons within 90 days after the close of the investigation, if he was notified while the investigation was continuing, or one year after being notified of the issuance of the summons, whichever comes first.

The Commission has tried to fashion protections for personal privacy without jeopardizing investigations in which the records of individuals are needed to establish the criminal conduct of a record keeper. If the individual is not the subject of investigation or is unlikely to be implicated publicly in any proceeding, government is not under a duty to serve such individuals when it subpoenas records. Cases of embezzlement or stock manipulation, for example, may require extensive analysis of individual account information to establish the illegal acts of the embezzler or manipulator.[96] Because such government access is not intended to produce action against the individual record subject, nor does it ordinarily disclose information in identifiable form, and because government does not usually retain account

[95] Testimony of Hon. Griffin Bell, Attorney General, United States Department of Justice, U.S. House of Representatives, *Hearings on Administrative Summons*, February 24, 1977, pp. 5-6; while the Commission understands the burden argument, it does not endorse the argument that an individual be given only one chance in any investigation to challenge government summons for his records, though the Commission is not opposed to the individual being required to challenge in the same proceeding a group of summons which were issued *at the same time.*

[96] The recently promulgated Federal Rules of Evidence reflect this need by providing for summaries of extensive business records, Fed. Rules Evid. Rule 1006.

CamScanner

information obtained for this purpose in its files, the Commission does not consider such access an unwarranted invasion of personal privacy.

The Judicial Subpoena in the Course of Litigation

There is considerably more supervision of subpoenas and discovery orders issued in the course of a law suit than of those employed in furtherance of an administrative investigation. The common law strictures on relevance and scope have retained their currency.[97] As with any government request for records, however, the individual about whom records are maintained by a third party has limited ability to intervene in any attempt to force disclosure. His interest may be somewhat better represented in the context of litigation than it is in the context of an administrative summons or Grand Jury subpoena, since the record keeper is often a party to the litigation and thus more likely to protect the record vigorously. Nonetheless, it is still a long way from control over records about himself. In this circumstance, there can be little argument that giving the individual notice and standing when records about him are sought will cause undue delay or other burdens. For these reasons, the Commission recommends:

Recommendation (4):

That Congress provide by statute that a subpoena or other method of judicial summons, issued after indictment or information or after the filing of a complaint or other initital pleading, issued to a private-sector record keeper

(a) in order to obtain an individually identifiable record and
(b) where the record subject is, or is likely to become, a target of the investigation, a named party to the litigation, or otherwise publicly implicated in the proceedings, may be issued only where
(i) service of the summons or subpoena is made upon both the individual identified in the record and the record keeper,
(ii) the individual has standing to contest the summons or subpoena and to halt production of the record until his claims are litigated, and
(iii) the individual is able to assert in protection of the record the defense provided by any legal expectation of confidentiality or other defense provided by common law or statute.

The Grand Jury Subpoena

Having dealt with the broad problems of summons and subpoena

[97] See, e.g., *Hecht v. Pro-Football, Inc.*, 46 F.R.D. 605 (D.D.C. 1969); *Richards of Rockfo Inc. v. Pacific Gas & Electric*, 71 F.R.D. 388 (N.D.Calif. 1976).

the administrative and litigation contexts, the Commission turned to the most powerful and perhaps most problem-ridden mechanism by which government can compel the disclosure of records.

> . . . The law vests the Grand Jury with substantial powers, because the Grand Jury's investigative powers must be broad if its public responsibility is to be adequately discharged. Indispensable to the exercise of its power is the authority to compel the attendance and the testimony of witnesses and to require the production of evidence.[98]

The flavor of the passage above suggests the great deference, often shading to veneration, paid to the Grand Jury. Included as a protection for the individual in the Bill of Rights, it is an institution whose unique powers the Supreme Court frequently reaffirms and protects. The first clause of the Fifth Amendment guarantees the Grand Jury process because it is viewed as "a basic guarantee of individual liberty," as "a barrier to reckless or unfounded charges," and, in crisis times, as a critical protection against abuse of the legitimate coercive power of the state.[99] In protecting the Grand Jury, the courts have rejected attempts to limit its traditional power of investigation on constitutional grounds.[100] Indeed, as Justice Powell noted in 1974, "the Grand Jury . . . has traditionally been allowed to pursue its investigative and accusatorial functions unimpeded by the evidentiary and procedural restrictions applicable to a criminal trial."[101]

All of which is not to suggest that the power of the Grand Jury to compel testimony and the production of evidence is without limits. The requirement that each person give what evidence he possesses is conditioned on that person's ability to assert a recognized privilege. But even constitutional privileges are not as absolute in the Grand Jury situation as they might otherwise be.[102] To return to Justice Powell's analysis, for instance: "Of course, a witness has no right of privacy before the Grand Jury."[103]

To balance these broad powers, the deliberations of the Grand Jury are theoretically protected by a strict standard of secrecy. The requirements of secrecy are designed to protect individuals into whose activities the Grand Jury may inquire. While the Grand Jury can acquire a great deal of personal and potentially embarrassing or damaging information, ordinarily it cannot release that information to the world unless it is prepared to indict an individual, to charge him with a particular violation of criminal law. If the Grand Jury is unwilling to accuse a person of criminal conduct, then it may not reveal the information it gathered.[104] Equally important, the Grand Jury has no adjudicative function of its own; its capabilities end with

---

[98] *United States v. Mandujano*, 425 U.S. 564 (1976).

[99] *Ibid.; United States v. Calandra*, 414 U.S. 338 (1974); *Costello v. United States*, 350 U.S. 359 (1956).

[100] *United States v. Mandujano, supra*; *United States v. Calandra, supra*; *Blair v. United States*, 250 U.S. 273 (1919); see also, *Branzburg v. Hayes*, 408 U.S. 665 (1972).

[101] *United States v. Calandra, supra.*

[102] See, e.g., *Rogers v. United States*, 340 U.S. 367 (1951); *Branzburg v. Hayes*, 408 U.S. 665 (1972).

[103] *United States v. Mandujano, supra .*

[104] See *Wood v. Hughes*, 173 N.E.2d 21 (NY 1961); *In re Talerico*, 309 NYS2d 511 (1970).

CamScanner

indictment or presentment, with an accusation that a crime has been committed. The Grand Jury gathers information, but can use that information only to determine whether the force of the criminal law should be brought to bear against an individual, whether there is "probable cause to believe a violation of law has been committed"; the Grand Jury does not determine final guilt or innocence, whether a man should lose his liberty or otherwise be punished.[105]

While there has been a great deal of recent criticism of the Grand Jury and its use by prosecutors, both at the Federal and State levels, the Commission accepted the constitutional existence and recognized powers of the Grand Jury in pursuing its inquiry. The Commission's concern is to protect privacy, to balance the preservation of that interest against the legitimate demands of society, not to reform the institutional structure of our legal system. It can not ignore, however, the threats to individual privacy in what it views as improper use of Grand Jury powers by prosecutors and government agents. The improper uses of power which concern the Commission are not so much deliberate attempts to violate rights or circumvent the law as abuses that stem from the "ordinary" operations of the Grand Jury—operations which are, in fact, quite extraodinary, as the following brief survey of the historical and theoretical foundation of the Grand Jury's powers shows.[106]

In medieval England, the Sheriff of each county empanelled bodies of twenty-three men, called "le grande inquest," to inquire into and present to the King's Justices the names of those believed to have committed criminal offenses. By the Fourteenth Century the function of the inquest was clearly limited to accusation; a separate jury and judge tried the accused to establish guilt or innocence. To secure the broadest range of inquiry for the Grand Jury and to assure that reputations would not be damaged simply because of inquiry or deliberation by the Jury, the jurors were pledged to secrecy. Indeed, that pledge of secrecy made no exceptions, even in favor of government.

The English migration to America brought with it the institution of the Grand Jury. In the first centuries of its existence in the new world it flourished. The Revolutionary generation especially revered the Grand Jury, using it to reject the initiation of prosecutions which the Royal government desired. As judges are fond of pointing out, the Grand Jury functioned as a bulwark of individual liberty. Its ability to protect subjects of investigation who were subsequently not accused was maintained; the duty of secrecy was jealously guarded. For these reasons, the Grand Jury was incorporated into the fundamental structure of the government of the United States in the Fifth Amendment to the Constitution.

As the Grand Jury emerged into the industrial age, particularly the

---

[105] *Supra*, notes 98-100, particularly *U.S. v. Calandra*; *People v. Johnson*, 203 N.E.2d 399, 401 (Ill. 1965); *Fed. R. Crim. P.*, Rule 6(e).

[106] The discussion in this and the following paragraphs is largely drawn from Blackstone, *Commentaries*, Vol. 4, pp. 301ff.; Wm. Holdsworth, *History of English Law* (7th rev. ed. 1956), Vol. 1, pp. 321-323; Kennedy and Briggs, "Historical and Legal Aspects of the California Grand Jury System," 43 *Cal. L. Rev.* 251 (1955); Dession and Cohen, "The Inquisitorial Functions of Grand Juries," 41 *Yale L.J.* 687 (1932).

CamScanner

Twentieth Century, its institutional structure began to change. Investigations of official misconduct, violations of anti-trust laws, and white-collar crime created a need for collectors and analysts of information to assist the Grand Jury in determining who ought to be accused of crime. Those who provided such assistance were government investigative agents and government attorneys. While they assisted the Grand Jury, they were not jurors and thus not clearly covered by the duty of secrecy, except with respect to testimony actually given before the Grand Jury. In addition to this new class of persons privy to some, or all, of the information before the Grand Jury, the Jury began to request frequently not only testimony but records as well. Documentary evidence was often essential if the jurors were to judge reasonably whether or not to accuse someone of a crime.

Out of these circumstances came the current operational structure of the Grand Jury. Its broad power to compel testimony makes the Grand Jury an unusually powerful means of conducting investigations and gathering evidence, particularly at the Federal level. Except for the search warrant, with its stringent requirements of probable cause based upon oath or affirmation, the Grand Jury subpoena provides the only form of compulsory legal process that can be employed for general inquiries into violations of law. The administrative summons cannot. Even without the measure the Commission recommends for constraining administrative summons power, an administrative summons can be used only to compel production of evidence germane to the purpose of the particular statute which granted the summons power—though, as explored earlier, the reach of such a summons can be overly broad.

In the Federal setting the United States Attorney (or his Justice Department counterpart) ordinarily makes all decisions as to what witnesses will be heard by the Grand Jury. Prompted by government investigators, he also determines what documentary evidence will be subpoenaed. As representatives of Federal investigative agencies indicated to the Commission, agents often seek Grand Jury subpoenas for documents on their own initiative from a U.S. Attorney to assist in investigations not yet brought to a Grand Jury's attention.[107]

It is the attorney for the government who decides when a Grand Jury subpoena will be issued and who issues it. The evidence gathered by the subpoena is then organized by government attorneys and Federal agents before being presented to the Grand Jury. Indeed, documents obtained by Grand Jury subpoena ordinarily pass through the hands of investigative agents who prepare reports for the government attorneys describing the contents of the subpoenaed documents. In most cases, a copy of such a report also goes into the files of the investigative agency. FBI agents, for example, prepare an "Agent's Report 92" describing the contents of

[107] Much of the material in this and the following paragraph is based on discussions with attorneys from the Department of Justice and U.S. Attorney's Offices and with Federal Investigative Agents, particularly interviews with Special Agents of the Federal Bureau of Investigation at Headquarters, Washington, D.C. on January 6, 1977, and at San Francisco Field Office on January 24 and 26, 1977; see also, *United States v. Cox*, 342 F.2d 167 (5 Cir. 1965); *Marston's Inc. v. Strand*, 560 P.2d 778 (Ariz. 1977); *supra*, note 100.

CamScanner

documents obtained by Grand Jury subpoena in certain organized crime investigations. A copy usually, though not always, goes to the strike force attorney, as well as to the investigative files of the Bureau.[108]

When documents obtained pursuant to a Grand Jury subpoena are presented to the Grand Jury, they, and presumably the information in them, come under the seal of secrecy. When documents are not presented, as often happens, however, they become part of an investigative record which some argue is not under the requirements of secrecy and thus is open to less restricted use by the government. In any case, the reports which are made part of an investigative file are not considered information maintained under the Grand Jury seal.[109] Even information presented and sealed is generally available to government attorneys and any Federal agents assisting them, though they may not disclose the information except by court order or in the course of criminal prosecution based on an indictment issued by the Grand Jury.[110]

In essence, the Grand Jury subpoena *duces tecum* has become little more than an administrative tool, its connection with the traditional functions of the Grand Jury attenuated at best. One might characterize its current use as a device employed by investigators to circumvent the stringent requirements which must be met to obtain a search warrant. Documents are subpoenaed without the knowledge, not to mention approval, of the Grand Jury. Documents summoned in the Grand Jury's name may never be presented to it. Indeed, the evidence obtained may not even reach an attorney for the government; it may simply be examined and retained by investigative agents for unspecified future uses. The unique powers of inquiry and compulsion, theoretically justified by the secrecy and limited effect of Grand Jury deliberations, have become a generalized resource for Federal investigative activities. Its broad use is underscored by a recent Justice Department internal memorandum which cautioned United States Attorneys and Strike Forces "not to appear to abuse the Grand Jury subpoena power . . . so as to furnish an excuse for adverse legislative action."[111]

The *Miller* decision provides a further example of how far the use of the subpoena has been separated from the actual functioning of the Grand Jury. In that case, the government attorney issuing the subpoena ostensibly on "behalf" of the Grand Jury, did not even pay courtesy to form; he stated as the return date of the subpoena a day on which the Jury would not be

---

[108] Drawn from a variety of interviews with Federal attorneys and investigative agents, particularly an interview with Special Agents of the Organized Crime Section, FBI, at Headquarters, Washington, D.C. on January 6, 1977.

[109] See, e.g., *Granbery v. District Court*, 531 P.2d 390 (Colo. 1975), where the Colorado Supreme Court stated that the policy of secrecy for Grand Jury proceedings "is intended only to protect against disclosure of what is said and takes place in the Grand Jury room," documents *per se* do not fall under the Grand Jury seal; also, *Marston's Inc. v. Strand*, 560 P.2d 778 (Ariz. 1977).

[110] *Fed. R. Crim. P.*, Rule 6(e); *Dennis v. United States*, 384 U.S. 855 (1966); also, *California Penal Code* §938.1 regarding release of Grand Jury information after indictment.

[111] United States Department of Justice, Memorandum of September 8, 1976 from Assistant Attorney General Richard L. Thornburgh to all United States Attorneys and Strike Forces.

sitting. In addition, the subpoena was served and the specified records obtained and analyzed by Treasury agents, not the U.S. Attorney or his assistants. Finally, as the Supreme Court pointed out, "the record does not indicate whether any of the bank records were in fact presented to the Grand Jury."[112]

The erosion of the protections built into the Grand Jury process to insure against improper and indiscriminate use of the information which comes before it disturbs the Commission. The broad powers of the Grand Jury can be justified only by the traditional protections in which its process was cloaked. The Grand Jury should not be a tool for collecting information which may be used for whatever purpose the government chooses; it should be a vehicle for specific criminal investigations. In order to assure against future abuse of the powers of the Grand Jury, the Commission recommends:

Recommendation (5):

That Congress provide by statute that a record obtained pursuant to a Grand Jury subpoena:

(a) shall be returned and actually presented to the Grand Jury under whose authority the subpoena was issued;

(b) shall be employed only for the purposes of prosecuting a crime for which an indictment or presentment was issued by the Grand Jury sitting at the time the record was obtained;

(c) shall be destroyed or returned to the record keeper if it was not used in the prosecution of a crime for which the Grand Jury issued an indictment or presentment or if it has not been made part of the official records of the Grand Jury maintained under the seal;

(d) shall not be maintained, or its contents described in any record maintained, apart from the sealed records of the Grand Jury by any agency or officer, employee, or agent of such agency of government; and,

(e) the information contained in such record shall be protected by stringent penalties for improper disclosure or maintenance, including penalties to be enforced by criminal prosecution (or the exercise of judicial contempt power).

In fashioning this recommendation, the Commission sought to avoid jeopardizing on-going investigations in which a Grand Jury about to expire has not issued an indictment. In such a case, the Grand Jury would be free to make a presentment to the judge, under seal or not, as it wished. The presentment would enable a second Grand Jury to continue the investigation. The Commission believes, however, that the recommended measure would effectively prevent government from using information obtained in a Grand Jury investigation for unrelated purposes. Indeed, to the extent the recommendation suggests the destruction and return of documents, the

[112] *United States v. Miller*, 425 U.S. 435 (1976); also, see the Court of Appeals opinion, 500 F.2d 751 (5th Cir. 1974).

CamScanner

Commission feels it will be particularly successful; information which is not available cannot be misused.

Having suggested the means for reestablishing and securing the traditional protections for an individual's privacy which should be part of the Grand Jury structure, the Commission does not believe it essential to extend the standards of notice and challenge it recommended for administrative summons and subpoenas in the course of litigation to every Grand Jury subpoena for records. In the administrative and litigation situations, to subpoena the record is tantamount to making it public. In the Grand Jury context, given the changes the Commission recommends, the fact of a subpoena does not necessarily mean the record will become public.

Even though the Grand Jury situation can be distinguished from the other forms of compulsory process, however, the Commission believes that the individual should be able to protect those records in which he has a legitimate expectation of confidentiality. The individual has rights even in the context of the Grand Jury; he may protect himself against self-incrimination, improper process, or the seizure of his private records. Since the records in which the Commission believes there is an expectation of confidentiality are ones which, were it not for the unprecedented changes in social and economic organization of this century, would be recognized as the private and protectible papers of the individual, the Commission feels that he ought to be able to protect those records from Grand Jury seizure just as he would from other government inquiries. For those reasons, the Commission recommends:

Recommendation (6):

That Congress provide by statute that a Grand Jury subpoena *duces tecum* (or other Grand Jury subpoena to acquire the contents of documentary evidence, whether by testimony or otherwise) issued

(a) to obtain an individually identifiable record,
(b) where a legally protectible expectation of confidentiality exists, such as the expectation recommended by the Commission for records of a credit grantor, depository institution, insurance institution, or health-care provider, and
(c) where the record subject is, or is likely to become, a target of the investigation, named in an indictment or presentment, or otherwise publicly implicated in the proceedings, may be issued only where
  (i) service of the subpoena is made upon both the individual identified in the record and the record keeper,
  (ii) the individual has standing to contest the subpoena and to halt the production of the record until his claims are litigated, and
  (iii) the individual is able to assert in protection of the record the defenses provided by any legal expectation of confidentiality or other defense provided by common law or statute.

Restricting Compulsory Reporting Requirements

Government requirements that record keepers, private and public, maintain additional records about individuals and report information from their records to government are increasing. More often than not, these requirements are designed to get information government legitimately needs—to provide health services, to assure against racial or sexual discrimination, to administer the tax laws, and the like.[113] Yet, this method of collecting information about individuals is fraught with greater potential for abuse, and threatens individual liberties and privacy more, than any other legitimate way government goes about gathering information.

The net of information reporting and record-keeping requirements is frequently spread wider than necessary; government finds itself with more information than it needs to carry out its responsibilities, and in a position to inspect or seize information which is not necessarily within its purview.[114] In addition, more record maintenance and reporting requirements inevitably mean greater government control of private-sector record keeping and, ultimately, more government control of information flow. Further, because much of the reporting and maintenance is mandated by the Federal government, but carried out by the States through federally funded activities, control of the information in government hands is centralized at the Federal level.

Progressive centralization makes access by government, particularly the Federal government, even less amenable to control. Traditionally, legal tools for protecting against government intrusion have checked neither the widening of the government's information net through reporting and record maintenance requirements nor the centralized control of record-keeping at the Federal level and the increasing ease of access by government to recorded information about individuals. The programmatic, piecemeal approach used to determine government information needs has not provided an effective forum in which to raise questions of whether government should seek as much information as it does or, indeed, whether there is some information it simply should not collect.

Perhaps the danger inherent in extensive information reporting and maintenance requirements levied by government is unheeded because its

---

[113] See, e.g., 2 U.S.C. 432 *et seq.* (regulation of election campaigns); 7 U.S.C. 136a (registration of pesticides); 12 U.S.C. 1749b (regulation of recipients of Federal insurance); 12 U.S.C. 1844 (regulation of bank-holding companies); 21 U.S.C. 355 (Food, Drug, and Cosmetic Act; licensing of drugs); 29 U.S.C. 431 *et seq.* (Labor-Management Act; regulation of unions and employers); 29 U.S.C. 626 (enforcement of age discrimination laws); 30 U.S.C. 821 (regulation of coal mine operators); 31 U.S.C. 1051 (Bank Secrecy); 42 U.S.C. 3769 (recipients of LEAA funds); 42 U.S.C. 299i (regulation of recipients of Public Health Service funds); 42 U.S.C. 300e-6 (regulation of recipients for health maintenance organizations); 42 U.S.C. 1786 (regulation of states and localities that accept Federal funds for nutrional assistance programs); 42 U.S.C. 1395mm (regulation of recipients of health maintenance organizations); 42 U.S.C. 2000e-8 (regulation of parties covered by Civil Rights Act); 47 U.S.C. 393 (regulation of recipients of funding for educational television and radio); Exec. Order No. 11246, 42 U.S.C. 2000e (regulation of parties who contract with the Federal government).

[114] See e.g., *Whalen v. Roe*, U.S. , 44 U.S.L.W. 4166 (1977); *EEOC v. University of New Mexico*, 504 F.2d 1296 (10th Cir. 1974).

CamScanner

specific elements have not been fitted together. The problem is not simply that government collects more information on individuals than it perhaps ought to; nor that the program-by-program method of granting power to collect information and then to judge the propriety of the collection is inadequate. Though these two elements must be understood to appreciate the dimensions of the danger, the problem is equally that the expanding reservoir of information government controls may be used for virtually any purpose once it gets into government custody. Information about individuals may be inadvertently or improvidently disclosed with consequent embarrassment or damage to the reputation of innocent persons. Perhaps worse, in a democratic society, is the ever present danger that someone in power may be tempted to use the information about individuals available to them for harassment or intimidation. In particular, government investigative agencies enjoy a unique ability to employ government's store of information about individuals with little restriction—most often for legitimate purposes but, as recent history reminds us, not always. The misuse of tax-return information by Federal investigators, for example, is well documented in all of the recent Administrations. The example, moreover, indicates that the pressure to engage in such activities comes as often as not from those charged with the oversight and management of investigative agencies.[115] Failure to appreciate that information frequently becomes a general governmental resource once it is in the hands of one agency, coupled with the failure to understand the dangers raised by the potential abuse of information in such an environment, is effectively illustrated by a recent decision of the United States Supreme Court.

The Flow of Information Into Government

On February 22, 1977, the Supreme Court upheld the constitutionality of a New York statute which required the reporting of every prescription for certain drugs and the inclusion of the reported information in a computerized central registry.[116] The specific purpose of the reporting and registry was to facilitate the investigation and enforcement of laws against the illegitimate use of narcotics. Patients, doctors, and two professional associations had challenged the portion of the statute which required that the identities of those receiving drugs be reported to the central registry. They argued that such reporting invaded the patient's privacy because the State had no need to maintain a record of the identities centrally. Indeed, during the first 20 months of operation under the statute with hundreds of thousands of identities registered, only once was the identification information relevant to an investigation of illegal activity. The challengers contended that the danger of improper disclosure and consequent damage to reputation, and the "chilling" effect of that danger on an individual's (or

[115] See, e.g., U.S. Senate, *Intelligence Activities*, pp. 115-116, 168, 181, 254-260, 280; a particular case in point was the ease with which FBI agents gained access to other government agencies' records on the Rev. Martin Luther King, Jr., U.S. Senate, *Intelligence Activities*, at p.220.

[116] *Whalen v. Roe, supra.*

doctor's) willingness to undertake drug therapy, was not balanced by sufficient public interest in the information to justify the central registry. The three judge panel which heard the case at the trial level agreed with the plaintiffs and found that "the diminution of a constitutionally guaranteed freedom is too great a price to pay for such a small government yield."[117]

Reviewing the lower court's ruling, the Supreme Court chose not to reevaluate the general issue of the constitutional propriety of requiring reporting of information about individuals for "legitimate" regulatory purposes.[118] Relying on past reasoning, the Court indicated that compelled reporting was to be distinguished from impermissible intrusions in violation of the Fourth and Fifth Amendments. The opinion noted that cases where intrusions were found illegitimate "involved affirmative, unannounced, narrowly focused intrusions into individual privacy during the course of criminal investigations" or circumstances where "there was an uncontroverted showing of past harm through disclosure."[119] The crux of the Court's opinion focused on the distinction it saw between the New York scheme and past schemes—the central *computerized* registry.[120] In assessing the threat to privacy created by the registry, the Court suggested that the considerations to be weighed were the dangers of "unwarranted disclosure of accumulated private data" and of inadequate "security provisions." In effect, the Court did not seem concerned with the intrusion created by collection but only with the potential for improper dissemination; even that concern seemed limited. Justice Stewart, in his concurrence, went so far as to suggest that the Constitution, to the extent it protects privacy, "does not recognize a general interest in freedom from disclosure of private information."[121]

Though litigants have long argued that reporting requirements imposed by government raise the same sorts of questions that would be raised by government searching your house or seizing your papers, their argument has carried little weight at the Federal level.[122] The Supreme Court consistently rejects it and restricts the reach of constitutional protections against government collection of information to certain limited aspects of reporting requirements.

Where the government requires an *individual* to report information about himself, the Court has found the Fifth Amendment protection against self-incrimination to provide some limitation on government power. In *Marchetti v. United States*,[123] the majority declared the wagering tax reporting system a violation of the Fifth Amendment privilege. As Justice Harlan reasoned for the Court, "The terms of the wagering tax system make quite plain that Congress intended information obtained as a consequence of registration and payment of the occupational tax to be provided to interested state prosecuting authorities." Since wagering was illegal in most

---

[117] *Roe v. Ingraham*, 403 F.Supp. 931 (3-judge Ct.)(S.D.N.Y. 1975).

[118] *Infra*, note 125.

[119] *Whalen v. Roe, supra.*

[120] *Ibid.*, at 4169-4170; also, see Justice Brennan's concurrence.

[121] *Ibid.*, at 4171.

[122] See, e.g., "Brief of Appellants Fortney H. Stark, Jr., et al.," *California Bankers Assn. v. Schultz*, 416 U.S. 21 (1974).

[123] 390 U.S. 39 (1968).

jurisdictions, continued the argument, such an intention amounted to a deliberate compulsion on a gambler to incriminate himself or be liable for failing to confess to illegitimate activity. Only a year later, however, virtually the same Court (with Justices Douglas and Black dissenting) refused to extend the rationale of *Marchetti* to the order form requirements of the marijuana and narcotic drug laws in *Minor v. United States.*[124] As Justice Douglas noted in his dissent, the issue was the same; the government had required an individual to report his own illegal activities or be liable for failing to incriminate himself. Indeed, the reporting forms which one needed to complete in the circumstances of *Minor* were never even prepared by the government—the statute was used solely as a prosecutorial "catch-22."

Though the standards of *Marchetti* and *Minor* may be difficult to reconcile, the broader protection given the individual under *Marchetti* is still quite limited. The *Marchetti* decision precludes compulsory reporting, and the use of information collected thereby, only when the mere fact of reporting amounts to incrimination. *In other words, reporting requirements are improper only to the extent that they leave an individual no choice but to incriminate himself.* In contexts where the reporting would not necessarily indicate illegal activity, reporting is proper even though compelled.

Where information about an individual must be reported by a *third party,* as in the case of the New York statute, the Supreme Court recognizes only the most nebulous constitutional protection. *The Court's only limitation on the scope of the reporting has been that the information be arguably relevant to the mission of the agency of government collecting it.*[125] This was the position the court took with respect to the New York drug reporting statute. Thus, even in the arena of medical or financial information (which most individuals consider peculiarly sensitive), the ability of government to compel reporting is restrained only by the requirement that information sought be "intimately related to . . . and obviously supportable as in aid of" an otherwise legitimate government activity.[126]

In the constitutional context, then, compelled reporting by government has been limited only to the extent that the reporting violates a narrow interpretation of Fifth Amendment protections against self-incrimination, or that the information sought is patently irrelevant to the proper activities of government.

The real danger to personal privacy from the vast store of personal information being accumulated by government is, in the eyes of the Supreme Court, the danger of improper dissemination. Preoccupation of the Court with questions of dissemination reflects its unwillingness to recognize the legal interest of an individual in records about himself held by third parties and its inaccurate understanding of how reported information may be used by government. The Court's approach, however, is understandable. By focusing on what government may do with information it has already collected, the courts have only to assess subsequent conduct on the basis of

[124] 396 U.S. 87 (1969).

[125] *United States v. Kahriger,* 345 U.S. 22 (1953); *Sonzinsky v. United States,* 300 U.S. 506 (1937).

[126] *United States v. Kahringer, supra.*

the actual harm caused by improper use or dissemination. Such an approach is judicially more comfortable than trying to assess possibilities and probabilities in advance, as they would have to do if they tried to judge the propriety of collecting the information in the first place and to balance the government's need for information against the individual's right to privacy.[127]

Unfortunately, individuals no longer possess all the records and information about themselves which they have a right to consider private. While the Supreme Court may be reluctant to recognize that bank account records, for example, are personal papers in which an individual has a legitimate expectation of privacy, society must give such recognition to those records if it is to preserve the delicate balance between the state and the individual. At least to the extent that an individual has a recognized and legitimate expectation of confidentiality, the Commission feels that third-party record keepers should not be required to report such information routinely. The same standard should prevail, in the Commission's view, even where the use of reported information is clearly limited and the dangers of abuse minimized.

The Flow of Information Within Government

To appreciate the relatively unrestricted flow of information within government and the dangers of that flow, the Supreme Court's consideration of the New York prescription reporting statute provides a useful starting point. In the course of its opinion, the Court assumed that the availability of reported information for purposes unrelated to the securing of "public health" would be restricted because the avenues for disclosure were restricted.[128] Restricted though the avenues for disclosure may appear to be on the surface of a reporting scheme, however, the availability of the information for specific investigative purposes generally opens up that record to law enforcement. The Court discusses "restrictions" on disclosure of drug users' identities by the State of New York; but, when an investigative agency legitimately obtains information for its investigation of a specific violation, such information goes into its files where the information is available when the same investigative unit inquires into other kinds of violations; and, the agents investigating possible violations of the New York drug laws were part of an agency which also investigates other violations of law. Further, the Court's reasoning does not take into account the routine cooperation and sharing of information by investigative units at all levels of government. Finally, the opinion fails to recognize that individuals have little, if any, power to protect themselves from improper use or disclosure *within* government.[129] In practice, then, government may require the

[127] See, e.g., *California Bankers Assn. v. Schultz*, 416 U.S. 21 (1974).

[128] *Whalen v. Roe, supra*, at 4168.

[129] Hearings before the Select Committee on Intelligence, U.S. House of Representatives, 94th Congress, 1st Session, pp. 977-79, 981, 1034-35, 1222-23 (1975); U.S. Senate, *Intelligence Activities*, pp. 254-262; also, see President's Commission on Law Enforcement and the

reporting of information for one purpose and use it for a second purpose—notably, criminal prosecution.

Equally important, the courts have found no constitutional limitation on the manner or extent of government disclosure of information about an individual, whether the disclosure is to the public, or to private entities, or within the confines of government. In the 1976 term, for instance, the Supreme Court ruled that there was no constitutional protection for an individual when a government official distributed copies of a leaflet which charged that the persons identified in it were "known" criminals, even though one of the individuals so identified had never been arrested or convicted of any crime.[130] Where the disclosure occurs between one agency of government and another, lower courts have held that there is no common law or constitutional restraint on such exchanges.[131]

While the implications of the free flow of information within government, particularly to or between investigative agencies, are described in Chapter 13, two aspects of that information flow must be considered here to determine how best to cope with the problems raised by government reporting and record-keeping requirements. The relatively unrestricted flow of information about individuals is endemic to both Federal and State government; the sharing of resources and the diffusion of authority and responsibility often require extensive exchange of information both within and between governments. The Commission recognizes the value of our existing architecture of government and understands that the very interdependence of agencies within the Executive Branch of the Federal government militates against unacceptable concentrations of power. The problem of intragovernmental information flow and public disclosure cannot be eliminated; but, the Commission believes that its dangers can be minimized.[132] Given the continuing danger of improper disclosure and use of information in government hands, the Commission believes it essential to limit requirements for the reporting of information about individuals maintained by third-party record keepers. Since the courts have made it clear that they do not feel it within their power to effect such limitation, any protection for personal privacy must be established by statute. Indeed, to the extent that protections against misuse of reported information or limitations on the scope of reporting currently exist, they are the product of legislation.[133]

That existing protections are the product of legislation is appropriate,

---

Administration of Justice, *The Challenge of Crime in a Free Society*, (Washington, D.C.: 1967), pp. 119-120, 266-267.

[130] *Paul v. Davis*, 424 U.S. 693 (1976).

[131] *Atchison, Topeka and Santa Fe Rwy. v. Lopez*, 531 P.2d 455, 467 (Kan. 1975); *Schulman v. N.Y.C. Health and Hospitals Corp.*, 355 N.Y.S.2d 782 (1975); see also Swan, "Privacy and Record Keeping: Remedies for the Misuse of Accurate Information," 45 *N.C.L. Rev.* 585 (April 1976).

[132] On minimization of these dangers, see also Chapter 14, "The Relationship Between Citizen and Government: The Citizen as Taxpayer."

[133] See, e.g., Tax Reform Act of 1976, 26 U.S.C. 6103; Census, 13 U.S.C. 9; Drug Abuse Prevention and Treatment Act, 21 U.S.C. 1102-1191; Child Abuse Prevention and Treatment Act, 42 U.S.C. 5101-5106.

CamScanner

since the problem of compulsory information reporting is the creature of legislation. In the past two decades, Congress has enacted hundreds of statutes which require, or permit, an administrative agency to require third parties to report information about individuals. As the Commission has found, it is futile to examine this problem as though each reporting requirement were an independent and unrelated scheme. Government is compelling record keepers to report information about individuals in unprecedented volume. In addition, the information reported covers a wider spectrum of individual activity than ever before, from health records to employment to financial activity. Most of that information becomes available for uses unrelated to the purpose for which it was reported. Even when government does not require reporting, it frequently mandates that records about individuals be kept and requires that they be open to inspection by government agents.

Record-keeping requirements for information about individuals are the statutory twin of compulsory reporting; ordinarily, when a record keeper reports information it must also retain that information. Further, statutes often require the retention of information which is not reported, but kept for possible inspection by government. Such record-keeping requirements raise many of the same questions as the reporting requirements. Government's access to the retained records is broad and virtually unassailable, particularly by the subject of the record. Even when legal process is ostensibly required for government to gain access to the records, such requirements provide little protection for an individual. Under the Bank Secrecy Act, for example, government agents may examine or seize account records without the account holder being able to object, even if the process by which the government proceeded was improper.[134] In other cases, Federal investigators have been permitted access to all the personnel and employment records of an organization, although they had no complaint justifying the examination nor any cause to believe that the records evidenced a violation of law.[135] Finally, access to records which are required to be kept by law may be predicated on statutory inspection provisions which exempt the investigator from obtaining legal process. Drug abuse control legislation, for example, states that government agents do not need a warrant to inspect books and records which the Attorney General (or his delegate) deems relevant or material to an investigation. This exemption from the need for legal process is provided even though the warrant in question is an administrative one which, under the statute, can be issued without probable cause. Such a warrant may be issued simply upon showing that there is "a valid public interest in the enforcement of this subchapter or regulations thereunder, sufficient to justify administrative inspections . . . ."[136]

The virtually unchallangeable power of government to gain access to records about individuals that a third party has been required to keep results, as do the reporting requirements, in information coming into government hands and becoming available for disclosure or reuse largely at

[134] *United States v. Miller*, 425 U.S. 435 (1976).
[135] *EEOC v. University of New Mexico*, 504 F.2d 1296 (10th Cir. 1974).
[136] 21 U.S.C. 880.

the discretion of government. Under most of the relevant statutes, a government agency has wide discretion to determine whether it will hold the information it acquires in confidence,[137] increasing still further the possibility of disclosure and future misuse.

Moreover, the Federal government does not limit the avenues through which it compels reporting of information or maintenance of records to direct requirements placed on third-party record keepers. Through a variety of programs, particularly those involving medical services and public assistance, the Federal government makes the States its collectors and record keepers by predicating Federal funding for State programs on fulfillment of such duties. Many of these funding schemes encourage, even obligate, State governments to collect more information about individuals than they otherwise would. The Medicaid program, for example, provides extra funding if the State agency administering the program agrees to adopt the Medicaid Management Information System (MMIS) information collection criteria.[138] Under them, medical-care providers must report detailed information on patients and their claims to the State authority. The extensive set of records then becomes available to Federal auditors or investigators, such as the newly created Fraud and Abuse Office in the Medicaid program, at their request. Predictably, given the financial incentives, most States have adopted the MMIS criteria.[139]

During the course of the Commission hearings on Medical Records, however, several witnesses testified that they do not consider the extensive collection of identifiable information mandated by programs such as MMIS necessary.[140] In particular, representatives of the Commission on Professional and Hospital Activities testified that there are viable alternatives to such massive reporting of information about individuals which would guard equally well against fraud and other abuses.[141] They advocated an auditing system by which the original records of the medical-care provider would be minimally abstracted and only that abstraction sent on to the Medicaid payer; the original record would continue to exist and be available for audit at any time; yet far less information would flow to government or any private insurer acting as a government intermediary.

Any reduction in the amount of information reported to government, such as the alternative to current practices suggested at the Commission's Medical Record Hearings, will correspondingly reduce the danger of abuse which inevitably accompanies the accumulation of information in government hands. The Commission suggests to the Congress, and to State

---

[137] e.g., 15 U.S.C. 1193; 7 U.S.C. 136f (trade secret); 15 U.S.C. 1944; 42 U.S.C. 1973g; 45 U.S.C. 362 (disclosable if it will aid individual); P.L. 94-106.

[138] 42 U.S.C. 1396(a)(3); 45 C.F.R. 250.90.

[139] Testimony of Medical Services Administration, Social and Rehabilitative Services, Department of Health, Education, and Welfare, *Medical Records*, Hearings before the Privacy Protection Study Commission, July 20, 1976, p. 218 (hereinafter cited as 'Medical Records Hearings").

[140] *Ibid.*, pp. 211-12, 222-23; Testimony of the Commission on Professional and Hospital Activities, Medical Records Hearings, July 21, 1976, pp. 462-65.

[141] Testimony of the Commission on Professional and Hospital Activities, Medical Records Hearings, July 21, 1976, pp. 462-65, 486-89.

CamScanner

legislatures, that they forego any future personal information reporting or record-keeping requirements unless a clear need for government to have the information exists, the need outweighs any privacy interest of the record subject, and there are no less intrusive alternatives for achieving the desired goal. In effect, the Commission believes that such an approach would result in statutes of greater utility and much less potential for harm than statutes like the drug reporting statute of New York State.

Not only are there extensive reporting and record-keeping requirements that make information about individuals available for government use, but few Americans are aware of the extent or nature of the identifiable information about themselves reported to government or kept at government's command. Some may know about one piece or another of the vast information requirements; but, those who begin to realize the breadth of information about them open to unimpeded government scrutiny are few. An individual has lost most of his control of what government can know about him. If the Bank Secrecy Act indicates the direction of future legislation, an individual may soon lose all control. The Commission hopes that legislators will recognize the impotence of the Constitution as currently interpreted to limit the reach of overbroad statutory commands to report personal information or to keep it on record. If they do, they will exercise extreme caution, particularly by limiting delegations of authority to executive officers to determine the scope of information reporting and the propriety of record inspection.

When reporting of individually identifiable information or the keeping of personal information are determined to be essential, the Commission recommends, in order to minimize dangers to personal privacy:

Recommendation (7):

(a) That where a private-sector record keeper is required to report information about an individual to an agency or authority of government, the scope of such reporting should be limited by Congress such that:

(i) each reporting requirement is expressly authorized in statute;

(ii) each statutory provision clearly identifies the policies and purposes which justify the reporting it authorizes;

(iii) each statutory provision details standards of relevance which must be met before the information must be reported;

(iv) no information is reported in individually identifiable form unless such reporting is essential to accomplish the statutory policies and purposes which justify the reporting; and

(v) where individual identity is not reported by the record keeper, yet at some point such identification may be necessary to ensure compliance with law, identifiable records be maintained by the record keeper only for

CamScanner

inspection by authorized agents of the government upon presentation of a lawful summons or subpoena;

(b) that inspection by a government agency of records maintained pursuant to statute or regulation in individually identifiable form by a private-sector record keeper be permitted to occur
- **(i) only upon presentation and delivery of a copy of an administrative summons, provided that**
- **(ii) the summons identifies the particular records and items of information to be made available for inspection by the agency;**

(c) that a private-sector record keeper be required to notify an individual when he enters into a relationship with the record keeper that information concerning the relationship
- **(i) will be reported to agencies and authorities of government pursuant to statute or regulation, or**
- **(ii) may be open to inspection by agencies and authorities of government;**

(d) that individually identifiable information obtained by government through reporting or inspection required by statute or regulation should be unavailable for civil or criminal prosecution of violations of law not directly related to the statutorily identified purposes which justify the reporting or inspection;

(e) that an individually identifiable record required to be maintained by a private-sector record keeper pursuant to statute or regulation may be destroyed by the record keeper at any time after the statute of limitations expires for the specific violation justifying the reporting or maintenance of such record; and

(f) that an individually identifiable record collected by a government agency from information reported or maintained by a private-sector record keeper pursuant to statute or regulation be destroyed by the government agency at the time the statute of limitations expires for the specific violation justifying the reporting or maintenance of such record.

While directed explicitly at the personal information reporting and record-keeping requirements of the Federal government, this recommendation is equally applicable to the actions of State governments. At the State level, however, the Commission recognizes that Federal requirements generate a large part of the demand for personal information. In consequence of that recognition, the Commission intends that the recommendation apply equally to Federal requirements levied on State agencies which result in private record keepers reporting to State authorities as well as to requirements placed directly on private record keepers.

Equally important, except for sections (c) and (e), the recommended measures seek to limit the reach of government power and assure the legitimacy of government activity, placing the primary burden for securing the protection of personal privacy on the potential invader, government, rather than the record keeper. Section (a) recommends clear statutory authority for reporting or record-keeping requirements, eliminating poten-

CamScanner

tially abusive executive discretion and providing in subsections (ii) and (iii) some standards through which the provisions of section (d) may be applied. Section (d) would permit government to take actions against fraud and other sorts of abuse within a program but would eliminate the use of records for unrelated purposes, *unless* Congress specifically provides in the authorizing legislation that the records ought to be available for other designated purposes. An example of such a provision can be found in the Tax Reform Act of 1976, which permits disclosure of tax-return information about a taxpayer provided to the IRS by a private-sector record keeper to Federal investigative agencies for use in non-tax investigations upon written request of the agency head. The Commission urges, however, that such deviation from the general rule be permitted rarely, if at all.

Finally, the requirements of sections (e) and (f) would eliminate records no longer needed for their original purpose but which in the future might cause the harassment or embarrassment of an individual. Records which do not exist cannot be abused.

Striking a Reasonable Balance

In August, 1973, Commissioner Donald Alexander of the Internal Revenue Service abolished the so-called Special Service Staff (SSS) within that agency and impounded its records. The SSS, established in 1969, accumulated information about American citizens whom the executive branch considered politically unwelcome, initiated IRS investigations and audits of them, forwarded information about them to other Federal law enforcement and intelligence agencies, and received information about them from other agencies that sometimes had been collected through illegal or improper means.

Testifying before the Senate Select Committee on Intelligence Activities in October 1975, Commissioner Alexander told the Committee that he had kept the SSS files so that the Committee "could review . . . them, and see what sort of information was supplied to us on this [sic] more than 11,000 individuals and organizations," adding that "at the end of all these inquiries, I would like to take those files to the Ellipse and have the biggest bonfire since 1814." Seconding Mr. Alexander's sentiments, the Chairman of the Committee suggested that "it might be a more important bonfire than the Boston Tea Party when it comes to protecting individual rights of American citizens."[142]

Commissioner Alexander's bonfire, and the abolition of SSS, highlight a basic element of the practices of government agencies that led the Commission to recommend the measures explained in this chapter. Alexander's suggestion that the SSS files be burned implicitly expressed concern about the vulnerability of information in government hands to abuse, while also acknowledging that government can, and does, collect information about individuals it does not need for any legitimate purpose, and thus should not have.

The recommendations in this chapter provide a means of curbing

[142] U.S. Senate, *Intelligence Activities*, pp. 95-96.

CamScanner

indiscriminate government collection of information about individuals, whether through informal requests, compulsory legal process or compulsory reporting. Allowing the individual a voice in government access to records about him and requiring outside supervision of government collection activities should create accountability for those activities, helping to assure that the acquisition of information by government is proper.

The Commission recognizes that its recommendations do not reach all recorded information about individuals, nor do they allow an individual to participate in all decisions as to whether government should have access to records about him. The Commission has concentrated on providing protections for the most revealing records of individual activity, the kind of records that government traditionally has been required to justify its interest in before they may be opened to it. Even where a legitimate expectation of confidentiality is recommended, government may still use a search warrant to acquire a record without the individual's prior knowledge. The recommendations, however, would no longer allow the executive branch of government to acquire records about individuals without supervision; no longer, for example, would unreviewed executive discretion enable government agents to seize an individual's bank records.

While appreciating the efficiency arguments of law enforcement agencies, the Commission does not believe that convenience alone should control policy judgments when individual rights are at issue. The burden argument, moreover, is not totally convincing. The IRS already, as a matter of policy, employs some form of summons or subpoena to obtain access to records.[143] In addition, the United States Department of Justice acknowledges that an individual should at least be notified when his bank records are summoned,[144] though the Department does not believe that a citizen should be given a protectible legal interest with which to challenge a subpoena or summons. In large part, the Department's position assumes the goodwill and good intentions of investigative agencies and their executive branch overseers. Such an argument, always unacceptable in theory, seems less tenable in practice in the aftermath of the Vietnam era and Watergate.

The law enforcement and investigative community has already indicated that it feels that some of the recommendations go too far; civil libertarians will undoubtedly be concerned that the recommended restrictions are not strong enough. The Commission, however, has sought to strike a reasonable balance between protecting personal privacy and assuring that the goverment can do its job. Just as the Constitution does not prohibit all searches and seizures, the Commission does not suggest that government agents be absolutely prohibited from obtaining records about individuals. Government, however, will have to make its case before it can do so.

---

[143] *Supra*, note 16.

[144] Testimony of Hon. Griffin Bell, Attorney General, United States Department of Justice, U.S. House of Representatives, *Hearings on Administrative Summons*, February 24, 1977, pp. 5-6.

CamScanner